

Tiger Team
Draft Transcript
June 22, 2010

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director

Good morning and welcome, everybody, to the Privacy and Security Tiger Team call. This is a federal advisory call, so that means the public will have opportunity at the end of the meeting to make comment. Let me do a quick roll call. Deven McGraw?

Deven McGraw - Center for Democracy & Technology – Director

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Paul Eggerman?

Paul Eggerman – eScription – CEO

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Latanya Sweeney? Gayle Harrell?

Gayle Harrell – Florida – Former State Legislator

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Carol Diamond or Josh Lemieux? Judy Faulkner?

Judy Faulkner – Epic Systems – Founder

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Carl Dvorak? David McCallie? David Lansky? Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Micky Tripathi? Neil Calman? Rachel Block? Christine Bechtel? John Houston? Wes Rishel?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Here

Judy Sparrow – Office of the National Coordinator – Executive Director

Sue McAndrew or Adam Greene? Joy Pritts?

Joy Pritts – ONC – Chief Privacy Officer

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

And Joy Keeler?

Joy Keeler – MITRE Corporation – Health IT Program Manager

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

This is what we get for opening right on time. Everybody is late.

David Lansky – Pacific Business Group on Health – President & CEO

Judy, David Lansky is here.

Judy Sparrow – Office of the National Coordinator – Executive Director

David, thank you. I'll turn it over to Deven and Paul.

Carl Dvorak – Epic Systems – EVP

Carl Dvorak is here too.

Judy Sparrow – Office of the National Coordinator – Executive Director

Thank you.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And David McCallie.

Judy Sparrow – Office of the National Coordinator – Executive Director

Thank you, David. Deven?

Deven McGraw - Center for Democracy & Technology – Director

I'm going to let Paul begin.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

Adam Greene just joining in. Sorry.

Judy Sparrow – Office of the National Coordinator – Executive Director

Thanks, Adam.

Paul Egerman – eScription – CEO

Good morning. This is Paul Egerman. Before I start, is there anybody else who hasn't announced themselves yet? Terrific. Good morning. Thank you for joining our tiger team conference call this morning. And to the members of the public who may be listening, we very much appreciate your interest in our work and your participation. Also to tell you, again very briefly, the tiger team was established by Dr. Blumenthal from people who were working in the standards committee and in the policy committee on privacy and security and on the NHIN workgroup. He wanted a small group of people to rapidly and aggressively address a number of issues, and that is what we are trying to do.

To make sure everybody understands the basic path that we are on, what we are starting with is directed exchange, the idea of a message that may be sent from one provider specifically to another provider, and some people have asked questions about why we are dealing with that. We wanted to do directed exchange simply as actually a simple learning tool to learn a basic format as to how to address issues,

then we will, starting in July, be working on a lot of more complicated environments and other methods of communications and issues with HIOs that aggregate data and retain data, and we will be dealing with some very exciting things starting in July, so this is just the first topic.

Now the way we are addressing this first topic is sort of on a dual path. The dual path is that based on some work that has gone on with a team headed by Arien Malic that's been working on NHIN Direct, they have seen some sort of like real world policy questions come up as a result of their work, and so answering some of those real world policy questions from a concrete implementation team has been one avenue of what we've been doing. The second avenue that's a parallel path is to address this issue from what I would call a policy framework approach. So that is the dual path.

On the dual path, on the first path on the concrete issues, I sent out a recommendation document that we prepared based on the meeting we had actually a couple of meetings ago. The recommendation document dealt with message handling and also dealt with credentials or digital certificates. A number of people have made some redlined comments on that. I know Dixie is on the call, and I very much appreciate your feedback, Dixie, and Micky Tripathi also made some comments, as did Adam Greene and David McCallie, all of which are extremely helpful.

What's going to happen is I'm going to sort of synthesize all that information and, later today, I will send out what I hope is either a final or near final version of the recommendations to everybody and give everybody sort of like a last chance to go through it. And just to sort of remind everybody of the rules, we don't want to wordsmith these documents in the conference calls. If people have any comments about the wording, they should handle that in e-mail because the more important issue is what are the fundamental concepts of the recommendations. The fundamental concept of the recommendation in message handling had to do with sort of the concept that, gee, the messages should be encrypted.

To the extent patient identity was known, that was like a tripwire that involves business associate agreements. To the extent that the message got changed, that was also like a tripwire that something else would happen in terms of contractual work. And the recommendations on the credentialing were important and interesting in that they start with the physician, patient, or the patient provider relationship and saying that's where the trust level needs to begin. So again, you'll get one last chance to look at that later today. We're going to ask everyone to respond by tomorrow because Deven and I then will present it to the policy committee on Friday.

When we did that entire process, I do have to say, going through the recommendations did give us a chance to learn something. I can tell you, I learned three things. One was I learned this is a terrific team. We have a great group of people. The comments that have been made are fantastic.

The second thing I learned is, as a group, we have an interesting challenge to find what I call the right technical level. Sometimes we're a little too technical, and sometimes we're not technical enough, and it's not easy to find that right technical level. It's sort of like being the porridge being too hot or too cold. But the challenge though is not only to find the right technical level, but to write our recommendation without a lot of technical jargon.

And the third challenge that we have is to simply keep on topic. We've got to keep very focused on the topic because as we try to solve every problem with privacy and security, we will not make progress. Those are the things that I've learned so far. SO the recommendation on that path that will go out hopefully one final time this afternoon. Unless anybody else has any comments, I want to turn the discussion to Deven, who is going to take us through our frameworks documents, and that's what we're going to try to accomplish today is to see if we can get through that before directed exchange.

Deven McGraw - Center for Democracy & Technology – Director

Does anybody have any further comments before I begin the second piece of our agenda?

Gayle Harrell – Florida – Former State Legislator

On the recommendations that did come out, Paul, we're not going to discuss those today? Those are, other than written comments, are not going to be discussed today? Am I understanding that correctly?

Paul Eggerman – eScription – CEO

That's correct.

Gayle Harrell – Florida – Former State Legislator

I just wanted to ask one question about that. When you're talking about unencrypted PHI, you are not – you did not put into the recommendations encrypted PHI. I was wondering, since you just made the statement that that was kind of basic that the exchange would be encrypted.

Paul Eggerman – eScription – CEO

That's correct. That's one of the wordsmithing suggestions is to clarify that. The assumption is that you're going to have encrypted message transmission. In the wording changes, we will make that clear that that is what is happening, and so that the rest of the whole thing happens. What happens when, in effect, there's a little bit of exposure along the way?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Paul, it's Dixie Baker. Both Gayle's comment and also a comment that Micky made in an e-mail, all of our write up really does refer to PHI, and as Micky has pointed out, that's really a HIPAA term for a subset even of identifiable health information. When we think about stage one transactions, there are other confidential transactions that are not necessarily even identifiable patient information like some of the quality reports that will go to CMS. I think we should consider just changing that to encrypted, sensitive information, or health information or something so that we be sure to consider that our recommendation applies to all kinds of transactions that include either confidential or safety critical information.

Paul Eggerman – eScription – CEO

I appreciate that. Then those are great comments, and so I do appreciate those comments. Deven?

Deven McGraw - Center for Democracy & Technology – Director

Well, I think, so one of the things that, as Paul said in the initial recommendations document, we're not – we have to be very careful not to try to boil the ocean here and to focus specifically on the questions that were teed up for us by the NHIN Direct technical team, which really doesn't so much have to do with the transmission of the data to CMS, notwithstanding that that's part of stage one of meaningful use, but that the transactions between messaging of patient data between two providers, largely for care purposes, whether it's direct treatment or care coordination.

And so I think that those messages, that those recommendations in that document are really targeted to those questions that arose, of which the handling of the reporting data that's part of stage one, I don't think that's really part of it, and we may need to parking lot that for later consideration. I just don't think we covered it. I mean, we have a really strong set of recommendations for those categories. If we try to take on too much in those sets of recommendations, we are going to jeopardize putting forth some very good work that is quite targeted to those circumstances.

Paul Eggerman – eScription – CEO

Yes. The recommendation does say in the very first sentence, this is for message handling between two providers.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

This is Carol Diamond.

Deven McGraw - Center for Democracy & Technology – Director

Yes. Go ahead, Carol.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

I have two, well, one comment and then a question. I'm wondering where these four categories come from. And the reason I'm wondering is for simple point-to-point exchange, shouldn't there be a policy conversation about whether or not to expose the data to anyone in transit before we get to trying to create policy for every possible approach to this? In other words, I guess I'm wondering why you need to expose the data in transit for direct exchange between healthcare entities. That's one question.

And then I just wanted a clarification on the comment, which was that the quality data is summary data. It's not individual data. So it falls into a different category, right?

Paul Egerman – eScription – CEO

That's correct. And to answer your question, Carol, these four categories were actually suggested by Micky Tripathi, perhaps at a meeting that you might have missed because I know we call a lot of these on short notice.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Yes.

Paul Egerman – eScription – CEO

We had a long discussion about it, and it does represent what we consider as the real world of how things currently work. And since it's the real world of how things currently work, it's appropriate to....

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

You know, I'm not so comfortable with that, and I'll tell you why. I think if we start to try to create policy for every possible technical approach to information sharing, this is going to be very complicated, and it will leave a lot of optionality on the table in terms of both standards and architecture. In my view, at least for this initial, simple, direct, provider-to-provider communication is it's unnecessary. There should be a constraint on this that says unnecessary PHI is not exposed in transit, period.

Paul Egerman – eScription – CEO

But what you're suggesting, Carol, it's unfortunate you missed the meeting. Maybe you and I could have a side conversation. But what's represented here is just the reality of how things work.

Deven McGraw - Center for Democracy & Technology – Director

Well, except that, Paul, we do make it very clear, and this is an important part of the recommendation to me. And if I'm overemphasizing it beyond where others in the group are, then we need to have a discussion about it. We recommend. We tell ONC that they ought to be, you know, to the extent that they're endorsing particular models of exchange and setting up standards for them, we say that models A and B that don't expose data are the ones they ought to be pursuing, and maybe we need to be stronger on that.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Yes, and I don't know that it's the reality. There are lots of ways to exchange data point-to-point, and there are some ways that expose it, and there are some ways that don't. And I think it's a policy decision and should not be a technical decision or a technical ease, you know, influenced decision. I also would say that the difference between A and B and C and D is significant enough to affect almost every policy in the rest of the framework. In other words, it's not just whether or not it's encrypted and how you use it. It starts to really affect most of the other aspects of the policy framework, and I do apologize that I was out last week. I feel very bad that I missed the conversation, but I'm nervous about going down this path where every option is on the table, and we have to come up with the sort of policy approach to options that are not cognizant or that don't implement the information policies that we're seeking.

Paul Egerman – eScription – CEO

Yes. I understand that, but the tough part is we did go through this all before. We actually had a three-hour discussion on it, and I think it's unfair to the other people to repeat that three-hour discussion. I'd be happy to talk to you about it separately, Carol, in terms of how it all turned out. And if you disagree, I'll report your disagreement on Friday when we do our report to the policy committee to make sure that your view is shown. But I think there are other issues relating to openness and transparency and consent that we have on our schedule, as we open up these four issues again. We'll spend all three hours talking about them again.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Yes, so the only thing I'm going to say is you can note that I disagree, and that all the issues around openness and transparency and consent are going to change significantly between A and B and C and D, and that will take much more time, but I'm happy to move on, so noted.

Paul Egerman – eScription – CEO

Thank you, Carol. You and I, if you want, we'll set up a time, and I'll make sure I understand what you're saying because I have a feeling, when we go through it all, and we start to go through the examples, I think you might feel a little better about this.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Paul, this is Micky. I'd be happy to join that conversation with Carol, if you and Carol think that would be helpful.

Paul Egerman – eScription – CEO

Yes. That'd be great.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

This is David. I missed that call too, and I wouldn't mind going through the logic because I think it's overly simplistic.

Deven McGraw - Center for Democracy & Technology – Director

You think what's overly simplistic?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

The four categories, I think that there's vagueness as to what an intermediary is, and I'm not sure it really matters in the long-run because, as Carol says, I think there's a high level policy that trumps all of it, but in a modular system where you have mix and match of things, I don't think it's going to be so easy to categorize real world systems into exactly one of these four buckets.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

I agree.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I mean, I think that they're broadly correct, and they communicate what we intend, so I'm comfortable in that sense, but I just think the details are going to get messy.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

I agree that there's a high level policy that trumps it all.

Joy Pritts – ONC – Chief Privacy Officer

Carol, what is the high level policy?

Paul Eggerman – eScription – CEO

Hold on a second. Here's what we'll do is I'll set up a call with Micky, David McCallie, Carol, and me, so the four of us, and we'll go through those.

Deven McGraw - Center for Democracy & Technology – Director

I should probably be on that call too, Paul, if that's possible. It's Deven.

Paul Eggerman – eScription – CEO

Let's make sure that we hit the agenda topics that we wanted to do. The comment that I have to say to Carol and David though is it's just not fair to the rest of us because you missed a call to make the whole team go through the whole thing a second time.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

No, I'm happy with that, Paul. I'm just saying, if we do have a remedial lesson, I'm happy to participate in the remedial lesson.

Paul Eggerman – eScription – CEO

I'm happy to hear everybody's feedback to that also. Deven, why don't we proceed with the frameworks document?

Deven McGraw - Center for Democracy & Technology – Director

Thanks, Paul. Just so people – Paul, you actually gave a terrific introduction about what the purpose of this is. But essentially the way I boil it down is to say we know that we need an overarching policy framework to support directed exchange. We've been working on and populating on the side a more detailed framework document when, on our last call when we tried to have a discussion about one piece of it, it very quickly got, not exactly off track, but it became a very unfocused discussion, which then led Paul and I to think about what might be a better way to frame this so that, again, we're not trying to boil the ocean with every possible issue. But instead, looking at the framework as applied to this very specific and narrow circumstance of directed exchange between healthcare entities.

And, in some respects, it assumes that there's the provider on the one end of it initiating that exchange to another provider who he or she likely has some knowledge of, and so again, that's a fairly narrow set of circumstances that is more related to an NHIN Direct type model. Therefore, a set of specific policies that you might need to layer in, in addition to the ones we already have in law, are not necessarily going to be the same as those that we might contemplate for exchange models that are much more complicated. And we're getting to those. But we're essentially trying this as an approach so that, again, we're sort of focused on this specific exchange model with the intent that whatever set of recommendations we come

up with in this conversation might actually help us, as we get the more complicated models, but we don't need to take all of that on in this conversation.

Essentially, the document that I'm talking about, just so I make sure that everyone has the correct one open is principle. The title is *Framework Applied to Directed Exchange*, and it starts with principles as applied to directed exchange between healthcare entities, and it starts with the first three, which are related: our individual access correction and data quality and integrity. And I'm actually going to suggest that since it was the individual access topic that took us a little bit off the rails in our last call that we start with number four, which is openness and transparency and try to move through the last sets of material: four, five, six, seven, and eight, and then do one, two, and three with whatever time we have remaining. And if we're not able to get to them, we'll have to parking lot them for another meeting.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Deven, I have just a quick question. Obviously what we're looking at looks very different from the framework table thing that a lot of us have commented on.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Does this reflect comments that we've already provided or is this...?

Deven McGraw - Center for Democracy & Technology – Director

Yes. I used that framework to make this document, but I pulled from it those pieces that I thought, again, were related to direct exchange between two healthcare entities. And so there are lots and lots of stuff that folks have added to the framework document that have to do with more involved or more complicated exchange models. But I did try to, I mean, that framework document is what I used to build this. But obviously not everything is in it, but I made a judgment call, clearly, and if there's something that you think is missing, we should talk about it. But it's that framework applied to this ... set of circumstances.

Paul Eggerman – eScription – CEO

And the reason, incidentally ... this is Paul, again, the reason that Deven produced this, and it was actually my encouragement partly to do that is we were actually surprised that we did not get more responses to the framework document. That we thought if we maybe narrowed it a little bit and surfaced some specific issues, we could generate more discussion. I appreciate your comments, Dixie, but unfortunately we didn't get a lot of other comments, and we really wanted to get some. That's one of the reasons why we reformatted it was to try to generate some....

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

No, I was just trying to establish the context here, and I appreciate it.

Deven McGraw - Center for Democracy & Technology – Director

Yes. We have not abandoned that, and for the folks who have added comments to that, they remain in the document, and we will continue to circulate it. I think it'll be much more actively used, as we get to the more complicated discussions in July.

Openness and transparency, and so the structure of this document, you'll see, is very similar for each category. It starts with the rearticulation of what the overarching principle is. This comes from ONC's principles that are also in the strategic planning document. There ought to be openness and transparency, and we know that the HIPAA privacy rule already provides us with a baseline here.

Providers have to provide what's commonly called the HIPAA notice, which there's definitely some commentary that it's not always terribly well understood. People sometimes think it's a consent form. It doesn't necessarily address what's the new environment. Certainly in conversations that we had previously with the larger privacy and security policy workgroup, we talked about how this transparency piece for patients is really important, even in directed exchange models. So there are three recommendations that we've teed up for your consideration here in terms of some specific policies.

One is that the Department of Health and Human Services and the extension, the regional extension centers develop guidance to help providers educate their patients about what's coming up that's new, which is electronic health records and electronic health records and electronic health information exchange, and what that means for patients. OCR, that's the Office of Civil Rights at HHS, should make clear in guidance that this is part of what should be in the HIPAA notice. And then the third piece, which ties to some of our other recommendation discussions, is where there are intermediaries with access to PHI, they ought to be transparent to providers about what they do with this, and this actually would refer to both PHI and deidentified data.

If you'd like, we can also talk about what providers ought to do with this information when they have it and whether that ought to be part of the disclosure to patients, but at a minimum, Paul and I, in teeing this up for your consideration, thought that providers ought to know, at a minimum, what intermediaries are doing with data. I'll pause there to let Paul add his two cents, and then we can open it up to discussion.

Paul Eggerman – eScription – CEO

Well, I mean, I think you've summarized that well, Deven. I think, in my opinion, the third issue is sort of like the headline that intermediaries should require to be transparent, so what we're saying is what's an intermediary? An intermediary is an HIO, but it's an organization like, say, SureScripts that takes the e-prescribing and reformats it and sends it through a retail pharmacy. They need to be transparency about what they do with that data. Do they retain it? Do they reuse it? Do they resell it? What do they do with it? HIOs allow them. Their business models are based upon reselling data, so that's, in my opinion, the headline.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Do you want to open it up for a discussion and questions because I have one?

Deven McGraw - Center for Democracy & Technology – Director

Go for it, David.

Gayle Harrell – Florida – Former State Legislator

Just a comment also when the line is formed.

Deven McGraw - Center for Democracy & Technology – Director

You're number two, Gayle.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think, Paul, I love that example, the SureScripts example because it was exactly what the question I wanted to ask, which is how far down the chain does the principle of openness and accountability back to, in this case, you say providers, but I would say maybe to patients also. How far does it go because obviously what happens to pharmaceutical data, from SureScripts it goes to the pharmacy? Then the pharmacy turns around and sells it to IMF and to other entities. Can the accountability go far down the chain? Is that something that we have any reason to talk about or think about?

Deven McGraw - Center for Democracy & Technology – Director

That's a really good question, David. I think, if we get – if folks are generally comfortable with the idea of having intermediary, you know, sort of the next, the one layer down, the entity that the provider actually deals with, and has a relationship with, having that transparency to sort of put that up as a recommendation. Then if folks were comfortable going farther than that, I certainly entertain it. It's a little hard to – I'm trying to conceptualize how we could hold sort of later stages down the chain accountable for that, but if that's something that we desire and we want to make that statement, it's a matter of this is something that HHS ought to consider, then I'd like us to get at least the one layer down recommended. If we can go farther than that, then I'm certainly open to it, but I want to make sure we can at least get to that point with the group.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Can I respond to that, or do you want to...?

Deven McGraw - Center for Democracy & Technology – Director

Do you mind, since Gayle got in the queue, and then we can keep it fair?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Okay, but I'm referring to David when it's my turn.

Deven McGraw - Center for Democracy & Technology – Director

Okay. Okay, Dixie.

Gayle Harrell – Florida – Former State Legislator

Keeping everybody in order, you need a whip. Let me tell you, Deven.

Deven McGraw - Center for Democracy & Technology – Director

People feel very strongly about these things, and we want to try to make sure everybody gets a chance to have their two cents. Go ahead, Gayle.

Gayle Harrell – Florida – Former State Legislator

I really want to address things from the patient perspective. I think that is the most critical thing we have got to do. We need the provider to have that transparency that the intermediaries must provide to the provider, but I think also the responsibility then goes down a level to the patient. Patients need to know what's happening with their data. It becomes very disconcerting to somebody to know that their personal health information, their very private health information has been sold to someone else for another reason. And that really, I think there needs to be very clear policy and when there is a HIPAA notification to patients that that is clear, in easily understandable language, that it's above a 0.6 type point, and that they understand that once that information goes through an intermediary, it may be sold to somebody, and they need to know that right up front.

Deven McGraw - Center for Democracy & Technology – Director

Thank you, Gayle. Dixie?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Now I'm responding to both Gayle and David because I totally agree with Gayle. I think the example that David gave, I have come to believe through other examples, is the biggest threat to really this whole EHR, NHIN we're trying to build is that when the whole paradigm is when a provider provides identifiable health information to a business associate for some healthcare operations and, of course, everything

under the sun falls into that. Then that we know happens, and it's included in the notice, and a business associate is in place, so assuming all that is in place.

What happens then is that business associate provides the data to the third party, either by selling it, by deidentifying it in some way and selling it, or repackaging it as limited data sets and making it available. The ... in my mind in neither here nor there, but it tends to make people more mad about it. And I believe that that second level of transparency, anything after the first one, needs to be at least visible to the patient and that they should have the ability to opt out.

Gayle Harrell – Florida – Former State Legislator

Absolutely.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Dixie, I hope you didn't interpret my question as implying anything other than that. That's where I was headed.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Put me on the list, please.

Gayle Harrell – Florida – Former State Legislator

Absolutely. I was just adding that that's what I think should be done.

Paul Eggerman – eScription – CEO

Just to bring focus to the discussion, this part of the discussion is openness and transparency. The opt out piece, we're going to talk about it in a minute when we talk about choice, but this is just openness and transparency. I'm not agreeing or disagreeing with you on the opt out; I just want to make sure the first piece is simple. Not necessarily simple--

Deven McGraw - Center for Democracy & Technology – Director

Thanks, Paul.

Paul Eggerman – eScription – CEO

--but the first piece is requiring that the intermediaries to disclose information, that's the first piece. Then we can talk about what might be done with that information.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I would further add that this should apply to research purposes as well where HIPAA has the ability for an IRB to waive the consent. I think it should at least be transparent....

Deven McGraw - Center for Democracy & Technology – Director

Right. That's all. Anything that HIPAA says today is arguably where HIPAA rules cover it, that's arguably got to be in the HIPAA notice. Then certainly there are some issues to resolve with making that more understandable to patients, but that I think that piece of it is covered in the rule.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

No, it's not. No, it's not. The HIPAA rule doesn't require that they tell patients that an IRB is waiving their consent.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

This is Adam. Can I clarify?

Deven McGraw - Center for Democracy & Technology – Director

Yes, please do.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

What HIPAA says is that I know privacy practices must include all of the 512 disclosures, which would be kind of the non-routine disclosures, which includes that your information may be disclosed for research. But that's simply that kind of the abstract that it may be disclosed for research. Dixie, you're right that there's no transparency as to whether in fact your information is being disclosed pursuant to an IRB waiver. The notice just says that it may be, so patients are notified of the possibility that their information could be disclosed for research. The notice doesn't give them details as to what that process is, and it doesn't specify whether it's happening in fact.

Deven McGraw - Center for Democracy & Technology – Director

Right. Also, keep in mind that this is the framework that's applied to directed exchange between two healthcare entities. And I certainly had the sort of initial stages of meaningful use in mind in terms of largely for care purposes, and we can make that more clear in order to keep these focused. Again, I don't think we can take everything on in this piece, but I think we can have some valuable things to say about a particular type of exchange that's called for in the early stages of meaningful use and parking lot these other very important issues.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Can I ask a question?

Deven McGraw - Center for Democracy & Technology – Director

Sure, Wes. Go ahead.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

For some purpose, my family practitioner sends information to a cardiologist at a university, and that cardiologist sends it to another cardiologist at another university, and that cardiologist, these two cardiologists aren't actually going to see me. Then that cardiologist has some waiver for an IRB and puts the data in the database. How much overhead are we going to allow for auditing the purpose and the waivers of multiple stops along the way in order to insure that the patient is apprises of everything that might go on?

Paul Eggerman – eScription – CEO

In response to that, Wes, I'm going to say those aren't the intermediaries. That's not directed exchange the way we're talking about it. We're talking about information at this stage going forward, point A to point B, and the discussion is what should the intermediaries disclose.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Well, if the doctor in the middle passes the information along, that's not defined as an intermediary?

What is an intermediary?

Paul Eggerman – eScription – CEO

Directed exchange means that one provider is giving information to another provider for a specific reason related to the care of a patient. So if it's a cardiologist, maybe that's a primary care physician referring a patient to a cardiologist.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

All right, well, let's assess my question just to that way.

Paul Eggerman – eScription – CEO

The issue is the cardiologist is not an intermediary. You're asking a question that's similar to the question David asked, which is, how far down the line are we going? The answer is we may want to go further down the line. But right now, the question is really about the intermediaries. It's the organizations like SureScripts or an HIO that may be acquiring the data. The question that you're asking, Wes, is an interesting one that we need to....

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Well, I mean, I'm glad to hear that you're not trying to impose a designer requirement that does N^2 or N to the N th power of combinations of here. That's very helpful.

Paul Eggerman – eScription – CEO

Yes. The issue that we're trying to do right now is just focus on the intermediaries.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

So an intermediary....

Paul Eggerman – eScription – CEO

This issue is a great question though.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

So is SureScripts an intermediary?

Paul Eggerman – eScription – CEO

Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

SureScripts provides value. That is, they return a list of the meds a patient is on to the original physician. They don't just pass information along. But they're an intermediary in this discussion, is that correct?

Paul Eggerman – eScription – CEO

That's correct, and so to the extent this discussion would apply to SureScripts, the proposal is SureScripts has to disclose to the providers and, as Gayle said, to the patients what they do with that data.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

So the requirement is that the husband and wife family practice that I use has to be sensitive to getting an update from SureScripts that says they've started to sell information and modify their HIPAA form them to include that. Is that the direction this is headed? Is that right?

Paul Eggerman – eScription – CEO

Well, the best way I can answer that is, if SureScripts is selling information, the direction this is going to is saying they need to notify their providers. Now what the providers do with that information is up to them. We haven't gotten to the issue of consent yet whether or not that influences – whether or not it has any influence on them. But the first step is the providers and the patients have a right to know that. At least that is the concept that is being put forward as a proposal.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Well, I mean, then I guess, so if I understand the concepts being put forth for proposal is the patient has the right to know that. The provider has an obligation to track that for all of the intermediaries that they send data through and correlate that information. That seems to be a logical consequence of the proposal on the table. Is that correct?

Deven McGraw - Center for Democracy & Technology – Director

Actually, I would not have said that we were placing an obligation on providers to chase that information down. I think we're asking for the intermediaries to be required to disclose it to the providers.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Right.

Paul Eggerman – eScription – CEO

Yes. I think that's a great distinction.

Deven McGraw - Center for Democracy & Technology – Director

So the burden is not on the providers to figure that out. That's certainly not.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

No. I presented my option a little differently. I said the provider got notified. Now is there a burden on the provider to reflect that notification in its HIPAA to notify the patient, or to have somewhere the ability for a patient to find all the intermediaries they use? Often they don't even know they use SureScripts. They use whoever their EHR vendor recommends

Judy Faulkner – Epic Systems – Founder

This is Judy. Jumping in to add to you, I think you've got the labs, SureScripts, billing companies, insurance companies, referral approval companies, and maybe even I don't know if you would consider this or not, but state immunization and public health. So I'm just expanding on what you're saying.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Yes, but those are endpoints.

Judy Faulkner – Epic Systems – Founder

Okay, so they wouldn't....

Paul Eggerman – eScription – CEO

But they may go through an intermediary like a clearinghouse.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

But the provider has a choice of either putting it in the notice or not using that as an intermediary.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

The baseline is that the provider has, I mean, where we are now is the provider has these vaguely worded notices that are essentially meaningless. As I understand the conversation, we're focused on sharpening that language and getting it to at least 6.1 type. The question that I think I'm asking is what is the obligation of the provider in order to insure transparency to the patient. Literally, the intermediaries can change in the course of the administrative work of the practice. The intermediaries themselves can

change their policy with regards to what they're doing. I'm just asking how this gets tasked back to the patient. That's all.

Deven McGraw - Center for Democracy & Technology – Director

Let me first make sure that we are at least onboard with the recommendations that we put forward in the document, which actually don't go so far as to say what ought to be disclosed to the patient, which I definitely heard this from folks who are interested in taking it to that point. But I want to make sure that we are clear, and we have agreement that, at a minimum, that information ought to at least be disclosed to the provider.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

This is Carol. I'm not there, and the reason I'm not there is the same reason I raised earlier. I don't know why we need to leave so much optionality on the table about what people can do in the middle in terms of examining and retaining and using the information, disclosure or not. I am really struggling with why directed exchange, point A to point B, requires the exposure that is unnecessary.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

It seems to me though that we want to be able to allow the flexibility to provide different levels of business service, and so all we're saying is that if that exposure is deemed necessary for a particular level of service that they're going to provide, there ought to be certain rules about that and, at a minimum, there ought to be transparency about the fact that they're doing that, rather than coming in with a policy that says you can't do that. I don't know how we would force such a thing anyway. We could confine ourselves from a policy perspective to just that very narrow definition that you're describing Carol, as a group. As you'll say, those other things also exist in the market. We're, as a group, not going to say anything about those. That will be one approach, but I don't think we can sort of just take a policy sweep and say they're not going to happen by....

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I think what Carol is saying that if you want to claim to be a directed exchange then, by definition, you don't retain information, period. You're something else. And so if you're something else, you don't – these policy rules are not the ones that apply to you. I think she's saying, going in, directed exchange should be defined. You don't retain information.

Paul Eggerman – eScription – CEO

Well, yes, but this is Paul. I mean, I think the reality is that it is getting retained. You look at the example of SureScripts.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I wouldn't consider them a directed exchange. I would consider them an HIE, but not a direct – you know, I think directed exchange, and maybe I'm totally wrong, but no, I'm not because this is what Deven defined it as just a while ago. She defined directed exchange as a point-to-point exchange between providers with clinical information.

Paul Eggerman – eScription – CEO

Yes, but look at the example of e-prescribing. The physician does an electronic prescription. The intention is to transmit it to the pharmacy, say Walgreen's.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

That's....

Paul Eggerman – eScription – CEO

But the way it may get transmitted is it goes through SureScripts.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Right.

Paul Eggerman – eScription – CEO

That's what happens, but your policy says that information should be known to the physician.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

To me, that's not a point-to-point exchange. That's two point-to-point exchanges.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

The question is, is SureScripts a provider or a business associate, and I think it's a business associate.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

Paul Eggerman – eScription – CEO

It's an intermediary. It's not a provider.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

But it is....

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I think the question is directed the way we've been using the term directed exchange, it would say that multi-endpoints are, I mean, I just see SureScripts as adding value over and above transferring information. The value includes a patient master index. The value includes retained data. It just doesn't sort of fit my model of what an intermediary is for the simple act of sending information to point A to point B.

W

I agree with that ... just got....

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I agree.

David Lansky – Pacific Business Group on Health – President & CEO

I agree. This is David Lansky. I agree too. I had one more distinction, I think, that is missing now. I think the case of pure direct exchange where NHIN Direct started is a very small subset of cases that are, as Deven defined them initially, point-to-point between known providers for the most part. Anything outside of that triggers this avalanche of complex issues that is really where the bulk of our work will inevitably be. Maybe we can define a set of policy constraints around NHIN Direct, but I think it's a small and simple task because of this Pandora's box problem. The middle case though is the routing and addressing that we talked about a little bit last time where the PHI is not exposed to the intermediary, but it's purely facilitating a point-to-point transaction. I'm not sure that's a real case either, but I think we could probably dismiss the pure NHIN Direct class of cases pretty quickly because they're few and simple. I don't think SureScripts falls into that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I would point out that that was the original provocation to create NHIN Direct was to carve out a pure and simple use case.'

Paul Eggerman – eScription – CEO

Yes, although that's not how NHIN Direct has evolved, and maybe it's because of the challenge we all faced about....

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I'm sorry. How is NHIN Direct involved?

Paul Eggerman – eScription – CEO

It includes all of these issues relating to intermediaries.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I don't....

Paul Eggerman – eScription – CEO

Let me....

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

How are you determining that, Paul?

Paul Eggerman – eScription – CEO

That's the way I understand it, but let me address this issue from a slightly different standpoint. Let's look at the second recommendation, which related to credentialing. The way the second recommendation works is that a provider is responsible for ascertaining the identity of the destination, making sure that who they're sending the message to is really the correct, authorized person, or correct, authorized entity. But then it says the provider, at their option, can delegate that. And so, one way a provider could delegate that would be a provider could say, well, the way I'm going to do all of my communications is I'm going to send all of my messages to my HIO, my health information organization, and have them send it to the right person.

They're going to be the ones responsible for making sure their certificates are correct and the identity is correct. That way I don't have to worry about that issue. That's something that would be a very logical thing for a small provider to do. And so it's sort of implicit, I think, in this type of recommendation. But in doing that, you create the environment where there is an intermediary, right, because of the HIO that is taking the message and then shooting it to whoever it belongs to. And so the question then is, well, in that process, are they doing anything else? Are they retaining any data? If so, they need to disclose it.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

But there's no current planned part of NHIN Direct that requires that they create that additional data or do anything with it, and the assumption is that they won't other than is necessary to maintain legal audit logs.

Paul Eggerman – eScription – CEO

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

On the other hand, SureScripts makes a business out of retaining that data and doing all sorts of things with it.

Paul Eggerman – eScription – CEO

Right, and it's a belief. It's not based on data. It's a belief that a lot of the HIOs will use data, selling of data as part of the business model.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

But that excludes them from NHIN Direct.

Paul Eggerman – eScription – CEO

Correct.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

What David just articulated is exactly what Carol Diamond is asking for is that assumption, what he called an assumption. It's also a policy that by policy, a direct exchange, NHIN Direct exchange does not retain data other than audit.

Joy Pritts – ONC – Chief Privacy Officer

This is Joy. I think it would be good to go back to David Lansky's original proposal, which was, he said that he thought that you could probably walk through the "pure" direct exchange parameters fairly quickly. And I think there are a lot of other issues to resolve, but it would be helpful to at least get those off the table, and then we can move on to some of the more complicated things. Can we do that?

Paul Eggerman – eScription – CEO

I don't know how to do that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

That's what we're trying to do.

Deven McGraw - Center for Democracy & Technology – Director

I have a suggestion. I actually think that that is a very good one, notwithstanding that the other document does note that there are other exchange models out there. That recommendations document also says that for directed exchange that the models where no data is exposed to an intermediary are the preferred ones. That's already in there, and that's clear, and if we jump off from that point and try to populate that framework, populate ... framework with that in mind, we can tick off a bunch of these very targeted recommendations without having to take on the more complicated models that we know are awaiting us in July, but essentially we think that there ought to be some, put some things in place, in other words, for the directed model that is our preferred best practice recommendation in our other document and parking lot for a later day this issue of intermediary access to data, which is in place in some of the more complicated models. Does that make sense?

Gayle Harrell – Florida – Former State Legislator

What you're saying is take out the recommendation number three out of that....

Deven McGraw - Center for Democracy & Technology – Director

Yes. Parking lot it. We go with the first two, some basic transparency about directed exchange without the data exposure per our recommended best practice, so that's right, Gayle.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

This is David. I'm going to ask a really dumb policy kind of question. It might make sense, and I think, from the point of view of people that are working on NHIN Direct, it would actually be welcome to actually define precisely what the policy constraints are in order to be called NHIN Direct. In order to participate in

something that has that name on it, you must meet the following criteria, the following policy statements. In other words, be proscriptive rather than descriptive. Is that something we can do?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

That's what we've been suggesting, I think.

M

Yes.

Deven McGraw - Center for Democracy & Technology – Director

Yes. I think that's what we're suggesting, David, and we're developing those. Here's what you should do. I mean, essentially in two documents. One is the specific set of recommendations that we're responding to people's questions, and then the second set is this application of the principles to that exchange model.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

That's good. It seems like we're allowing though for ambiguity around, we suggest that you not use the data for secondary purposes. I would say we just go and say if you use data for secondary purposes, you are not direct exchange.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Right.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

I would agree with that because I was going to suggest, Deven, that we get away from this idea that we prefer categories A and B. Rather, what we're saying is that, as David is saying, that if you want to call yourself NHIN Direct, this is the policy box you have to live in.

Gayle Harrell – Florida – Former State Legislator

That's all I was after.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

Gayle Harrell – Florida – Former State Legislator

...NHIN Direct, the examination, retention, and use of data in the middle is not necessary.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Or allowed.

Paul Eggerman – eScription – CEO

It's just impractical though is what I'm saying.

Deven McGraw - Center for Democracy & Technology – Director

But I'm not sure it is, Paul. I mean, those are the very models that we've already identified, which is the non-exposure of PHI to the – of unencrypted PHI to the middle.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

We've worked pretty hard to define a technical infrastructure that makes that feasible, makes this policy box feasible, so I think it's technically feasible. A business question, maybe that's different.

Paul Eggerman – eScription – CEO

So then we do have to go back to the recommendations and alter them, right?

Deven McGraw - Center for Democracy & Technology – Director

Except that, Paul, that's why I thought we were already there that ONC, I mean, we didn't actually, so I stand corrected. It was not articulated as it just clearly was that Micky and David articulated that if you want to be in the NHIN Direct box, then there isn't exposure to data.

Gayle Harrell – Florida – Former State Legislator

Correct.

Paul Eggerman – eScription – CEO

All right, but there's a difference between, first we've got to make a difference between directed exchange and NHIN Direct. Those are two different concepts. In other words, you could do directed exchange without doing NHIN Direct, right, because NHIN Direct is a set of standards. But you can decide you're going to do directed exchange. You don't necessarily have to use those set of standards.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, I would agree that NHIN Direct is a particular, perhaps branded way if you would.

Paul Eggerman – eScription – CEO

It's a branded way of doing things.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Paul, my point is that you are going to choose the standards that fulfill these policy constraints only if the policy constraints exist. If they don't exist, then the world is open to how you accomplish directed exchange, and you could do it any number of ways using information in the middle.

Deven McGraw - Center for Democracy & Technology – Director

Paul, I think there would be high value, actually, for us to define that policy box for NHIN Direct since it's on the table. And to kick off, in addition to answering the questions, certainly some concept of direct exchange that is different from NHIN Direct, I'm not necessarily disagreeing with that, but since ONC is putting time and energy and money behind a particular exchange model that they're calling NHIN Direct, I think there'll be high value to defining that with some clarity.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think that if that – I want to pick back up on this notion of a brand, and I'll put brand in quotes because I don't know that ONC is going to produce a brand. But it would be possible to imagine where if one goes through a certain well-defined policy process and obtains an NHIN Direct address, then one can be guaranteed that they can refer to that and say that I use or I participate in NHIN Direct, and that that means certain things around protection of the data, as it moves from place-to-place.

Paul Eggerman – eScription – CEO

Let me just ask a question then. Why did ONC give grants to all these HIEs ... NHIN Direct, what does the role of the HIE have?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

But they're dealing with....

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Can I address that?

Deven McGraw - Center for Democracy & Technology – Director

Sure. Go ahead, Wes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I'm of course, if Joy wants to pick it up, I'm happy to let her do it. I was just going to talk generally about the difference between an HIE and NHIN Direct. Joy, do you want to take that?

Joy Pritts – ONC – Chief Privacy Officer

Why don't you take the first crack, Wes, and then I'll jump in.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

All right. You can deny anything I say. The services that are mandated for an HIE are substantially more complex than simply this directed exchange. They involve issues that we know are going to be on our agenda, but are temporarily off the agenda because of the limited scope of NHIN Direct. It appears that there is a need for both levels of service.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

One, that level of service that can be rolled out more quickly because there is less technology involved in fulfilling the policy requirements, and the one that adds more value because there is more investments, both in technology and time and consensus and legal agreements and setting up the policy necessary for retaining data.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

I would add, and maybe this can help clarify the conversation, maybe, that we can separate. I think we're lumping together organizations and the functions that they perform, so to take the SureScripts example, they could have an NHIN Direct set of services that are NHIN Direct — approved" that are separate from what they do with respect to data retention. And so the organization can have a set of functions that they roll out that are isolated in order to get that NHIN Direct branding to the extent that they find that valuable and there's market for it. And just because they retain data for other purposes for other transactions is a separate consideration that all happens in the same organization, so ... separate out the organization.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think that's a good point, and I think that is in fact their intent.

Deven McGraw - Center for Democracy & Technology – Director

But to the extent that they're using the direct model, then I think what I'm hearing being said is that they aren't retaining data ... model.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Yes, and to the extent....

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

For those transactions.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

For those transactions, correct.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Yes, to the extent of transparency, they have to be able to create a disclosure to practitioners that identifies which services or companies fall under the NHIN Direct model and which are value added services that use a different. I think, frankly, they use a business associate agreement all the time.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Right, and provide enough representation to their customers that they, from a technical perspective, have isolated those transactions so that they're not getting mixed up within their own infrastructure.

Gayle Harrell – Florida – Former State Legislator

I'd like to add that they also need to have very distinct policy on each level and make it very clear to the provider that when it is direct exchange and only direct exchange, they are under this set of policy guidelines. But when they move over to that intermediary or changing data or aggregating or whatever, that then they have to meet another set of guidelines, and that they're very, very clear which is which. Also, it needs to come back down, and the patient at some point needs to know when an intermediary is involved and there's potential for all kinds of things to go on. The patient needs to know that too.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

I think that's where this can be incredibly valuable to the market in that, to the points earlier, it's hard for physicians to sort out all of these different levels and to really understand that particularly when there are a number of transactions that start happening out of a number of different types of transactions coming out of their EMRs. But if there is a common, well-understood understanding with branding and enforcement of some level around NHIN Direct, at least everyone then has a degree of assurance that if something is branded NHIN Direct, there are limitations on what can be done with that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think that makes a lot of sense.

Paul Eggerman – eScription – CEO

Yes, but I just feel that I understand what you're saying, Micky, and I think it does certainly make sense. But our policies should not be limited to NHIN Direct. We need to have policies that cover the general case, especially since NHIN Direct doesn't really exist. While the policy is evolving, people are exchanging data right now. And we need to have answers to some of these questions.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Paul, this is Dixie. I think that what we're talking about here is beyond exchange of any type. I think where we've wandered into is the realm of limitations on what a business associate can do with the data that's entrusted to them for healthcare operations, besides what they're on contract to do because any business associate, if you're on contract to do X, there should be constraints placed on what else you can do with those data. I think that that's really a critical, critical issue for this group to address, but I think it's not an exchange issue. I think we're lumping too much around exchange and intermediary when we should be talking about here's a simple, point-to-point exchange of data. And, over here, let's talk about constraints on business associates.

Deven McGraw - Center for Democracy & Technology – Director

Yes. Dixie, this is Deven. I think I'd phrase this slightly differently, but I think I'm making the same point, which is to say to Paul, certainly these other exchange models that we've spent some time carving out

and identifying that involve intermediary access to data do need to get addressed. But to the extent that we sort of agreed that we would start with the simple point-to-point exchange for our set of recommendations for this month, I think we can and should be that narrow and be that clear and then move to those others.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

Paul Eggerman – eScription – CEO

Getting back to the frameworks document, does this mean we're just dropping the recommendation about intermediaries having to disclose?

Deven McGraw - Center for Democracy & Technology – Director

Yes. We're parking lot it. I like it, but we don't need to address it with this set of recommendations for June is what I'm suggesting.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Because we would basically say they may not disclose if they want to be direct?

Deven McGraw - Center for Democracy & Technology – Director

They may not collect. They're not having access.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I'm sorry. Yes. May not collect, other than for legal auditing purposes that's required by ARRA and so forth.

Deven McGraw - Center for Democracy & Technology – Director

Right. Just let me make sure. When you say other than is required by legal auditing purposes, you're just talking about auditing that they perform the function from point A to point B?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes. Yes. They may be required to keep logs for other reasons, but those logs are just for auditing purposes, not ever processed for any other use case.

Deven McGraw - Center for Democracy & Technology – Director

Right, and if there isn't identifiable information exposed in the transaction, then it shouldn't be in the audit log either.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I would say that's correct. It probably just is, I sent a message from A to B.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Right. The ARRA statements that you've made there, this is Dixie, we're not including accounting for disclosures, which is considerably more than audit, right? The intermediary should not be providing the additional service of helping the covered entities account for disclosures.

Deven McGraw - Center for Democracy & Technology – Director

No, that's a completely different topic, I think.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Right. But he talked into ARRA, so I want to make it real clear.

Deven McGraw - Center for Democracy & Technology – Director

It sounds like we're ready to move on to individual choice.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

Deven, this is Adam. Before we move on, I want to discuss the OCR recommendation.

Deven McGraw - Center for Democracy & Technology – Director

What OCR recommendation? Okay.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

OCR should make clear guidance that is part of the HIPAA notice requirement.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

I take it to mean that that's providing transparency about electronic health information exchange is part of the HIPAA notice. Is that what you're...?

Deven McGraw - Center for Democracy & Technology – Director

Yes, that's what we were suggesting. Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Deven, it's something other than six points type.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

At least seven points.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

I'd like to clarify on that front that we can provide guidance that interprets the regulations, but we can't go beyond the regulations in guidance. So here are a few options that might help this get more tailored to what we can actually do.

Deven McGraw - Center for Democracy & Technology – Director

Okay.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

Option one is that right now our regulations do not require that the notice address electronic health information exchange. You have to provide examples of treatment, payment, and healthcare operations,

but we don't specify what those examples are. So option one would be suggesting that we change the regulation to require that electronic health information exchange is addressed. Option two would be that we promote as a best practice that the notice includes electronic health information exchange, so that wouldn't be guidance in that it's not interpreted ... and we can't require it, but we certainly could try to promote it.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

We could include both of those in our recommendation, right?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

You could include both, yes. I just was weary of a recommendation that we provide guidance, which would suggest that this is what the regulation says when the regulation in fact does not currently state that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Could you repeat choice number one again? I just didn't hear the last part of your sentence. You said change the regulation to require that--?

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

To require that the notice address electronic health information exchange.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I got it. Thanks.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

And option two would just be to not change the regulations, but to promote it as a best practice.

Deven McGraw - Center for Democracy & Technology – Director

Those are helpful. I mean, I personally would like to list them both. I think the most important thing coming out of this group is that there ought to be transparency about that, and it's really up to the agency to figure out how to get that done effectively.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

Okay.

Deven McGraw - Center for Democracy & Technology – Director

But we don't have to phrase it in terms of guidance because that does suggest that there's something that you could do. As you've just explained, there might have to be some other actions taken, but I think our goal is to say that there ought to be transparency about this patient.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think an interesting question in terms of what you can and can't do from what the government can and can't do would come back to this notion of what we were calling a brand. If certain explicit policy constraints were defined that perhaps do in fact go beyond regulations and were simply associated with that brand or that name, is it possible to endorse ONC, for example, to endorse that brand and say, you know, you may use this only if you meet these constraints, even though it's really not in the regulations,

per se. It's just kind of a stamp of assurance. Is it worth pursuing an angle like that in the long run? Is that completely unheard of?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

This is Carol. I'd be curious what Joy and others think the answer to that question is, but I feel like we're kind of down the same path on the standards side. There are certain standards in the IFR, but the standards that are going to be used for NHIN Direct are simply standards specifications that are going to be released. And I think, similarly, these are policy specifications that are going to be released that fulfill the objectives of the law, but I'm curious about the official answer.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

This is David. I'll just push the use case slightly further. It is completely feasible technically that in order to participate in NHIN Direct one must obtain a certificate that routes back to a government approved entity.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

So you could actually control it and say you technically can't participate unless your process leads to a certificate that you obtained from a government defined entity, so you could make it quite precise as to what it means to be a participant in NHIN Direct. The question is, can the government do something like that?

Joy Pritts – ONC – Chief Privacy Officer

This is Joy. Right now, NHIN Direct is a pilot project, and there are – in order to mandate certain things, it's quite likely that it would require regulations or probably the Administrative Procedure Act. So at some point there will be a reevaluation of the pilot project as to what recommendations come out of, both policy wise and technology wise. But at the current point, it is a voluntary pilot project, and because it is a voluntary project, we will not be, at this point, mandating certain things because doing so may put them into a more concrete form than most people would be happy, so we need to maintain this as a pilot project. It's voluntary. The people who participate in the project will voluntarily say that they will follow certain things. If they don't, then they're not part of the project. After the project is over, there will be an evaluation period to see where the technology and the policy decisions need to start moving.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Isn't the intent ultimately, I mean, if it works out ... this project, that it ultimately would be one way to participate in the NHIN Exchange without implementing NHIN Connect, in which case it would be governed under the same DURSA as the NHIN Exchange?

Joy Pritts – ONC – Chief Privacy Officer

I do not know the answer to that, Dixie. I do know that ultimately – we are ultimately looking for an NHIN, not – with policies that govern different modes of exchange and that the name of Direct as the policy project ultimately will go away.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Right.

Joy Pritts – ONC – Chief Privacy Officer

That is one of the reasons why we are trying to focus on more on the means of exchange and the characteristics of those exchanges than the particular projects involved because the policy recommendations that you're making should guide this project, but should also be applicable hopefully beyond the project. I know that's a hard level to get at. It's kind of ... mid stage there, but that's what really is most helpful.

For example, when the recommendation is that if there is an entity that is facilitating exchange or is in the middle that has direct access to PHI in some form that there need to be some limitations on what that entity can do with that information. That type of a recommendation was helpful from both the NHIN Direct perspective and in a more general perspective. It's what they call in the research world that term generalizable. It can be....

Deven McGraw - Center for Democracy & Technology – Director

Joy, this is Deven. I think we're definitely going to get there, but I'm also hearing on this call that folks want to create a set of policy constraints that apply to this pilot project involving, because the direct exchange from one point to another ideally should not involve access by the intermediary to data. We understand and have talked about the higher level models where that access may be necessary to perform a value added function, and so we're definitely going to get there.

Paul Egerman – eScription – CEO

But, Deven, in the pilot project, every single example of their work involves an intermediary, every one of them.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

But the intermediaries aren't retaining any data.

Paul Egerman – eScription – CEO

How do you know that?

W

Right, there's no exposure.

Deven McGraw - Center for Democracy & Technology – Director

The exposure piece is the key to me. It's not the data retention. Once the exposure happens, then you want to get to the retention policy and make sure it doesn't get retained. But I thought that I heard, and we did say in those recommendations it has always been there that the models that don't expose data are the ones that ONC ought to be pursuing for directed exchange ala NHIN Direct.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

I think that's the answer to your question, Paul, of how do we know that. It's actually the flip of that is that what we want to do is describe the policy box that says if you call yourself NHIN Direct, you have to fit into that box, which means that you don't expose it.

Paul Egerman – eScription – CEO

But my question is, if you call yourself NHIN Direct, is there an intermediary, or can there be an intermediary?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

This gets back to the question of what is an intermediary. So in the NHIN Direct rubric, there is something called a HISP, a health Internet service provider. The HISP operates on behalf of a sender or

a receiver to actually package up the message, encrypt it, and send it. But that HISP could well be a different entity in the community. It might not be the EMR vendor. It might in fact be the state HIE. It might be a third party company.

Paul Eggerman – eScription – CEO

So then you're saying NHIN Direct can have an intermediary.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Yes, but the question is not can there be an intermediary. The question is, is the exposure...?

Paul Eggerman – eScription – CEO

What can it do?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Right. Is exposure of PHI necessary? The answer to that is no. So whether or not there's an intermediary, what we're saying is there's no need to examine, expose, or retain the PHI.

Paul Eggerman – eScription – CEO

With the caveat, just, I hate to bring technical details in, but this is....

Deven McGraw - Center for Democracy & Technology – Director

But you're about to.

Paul Eggerman – eScription – CEO

But I will because tomorrow we're going to make a consensus agreement that this conversation could completely shoot down, and I don't want to go through the whole meeting tomorrow if this conversation is going to shoot it down. So the current consensus allows for a trusted intermediary, the HISP, to do the encryption on behalf of the provider so that the provider doesn't have to worry about public key infrastructure on his desktop.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, that's our second recommendation. The provider doesn't have to worry about that.

Paul Eggerman – eScription – CEO

Right, and so I don't want us to exclude that, or if we do exclude that, it means that NHIN Direct goes back to the drawing board.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I don't. This is Dixie Baker. You know, in the document, Paul asked for some examples, and so yesterday I tried to add some examples. And it became abundantly clear to me exactly what David was pointing out. What's an intermediary? Because whenever you use the Internet or Internet protocol, whatever you're sending from point A to point B will in fact go through a number of servers that will at least look at the routing information and will at least add another address to that routing header. By definition, that's the way the Internet works. So we are tossing around the term intermediary, and I think we really need to define it.

I would also point out that at any of those servers that that e-mail, whatever, goes through on the Internet anywhere, it can see the entire payload. So if it's unencrypted, it can see it. So if it goes through anywhere, any server, anywhere, people can sit there and watch the mail go by, so you can't just discount

e-mail servers that things go through or IP servers, whatever we want to call them because that's the way Internet works.

Paul Eggerman – eScription – CEO

We do encrypt the channel in the proposal, so once it leaves that trusted HISP, it is invisible.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Can we just do an agenda check. I'm a little confused. What is the topic we're talking about right now, Deven?

Deven McGraw - Center for Democracy & Technology – Director

Well, I mean, we are talking about removing from openness and transparency into individual choice, Paul, but I also think we're clarifying what our model is to which this framework applies, which is to the directed exchange where if there is something in the middle that is assisting in that routing, they don't have access to individually patient identifiable data in order to do that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Okay. That...

David McCallie – Cerner Corporation – Vice President of Medical Informatics

What I wanted to do, I just want to make sure because I don't want to get too far deep into the technical stuff about how the Internet works because that's a low level, it's extended to the intermediary, certainly what I would call a low level intermediary. The issue is, first, is there in directed exchange, is there an intermediary? The answer I'm getting is yes. There is an intermediary or there can be an intermediary.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

There will be, period.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Pardon me?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

But I think we should capture what Deven just said as policy that if any entity that assists in the routing of the traffic of the message from point A to point B cannot see unencrypted patient data.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

As David has just said, we have considered the special case ...intermediary that in fact provides the encryption service. And if the policy is simple, as you state, then we're just shot out of the water.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes. It seems to me, and I agree, I mean, the two questions I was going to ask is, is there an intermediary, and does intermediary ever see unencrypted data if there is one? It seems like the answer to the first one is yes, there is an intermediary.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

But if people are saying the intermediary may never see unencrypted data, I agree, Wes, everything is shot out of the water. I mean, the recommendation that this group did that spent 3.5 hours on, we just show that away and NHIN Direct....

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

No, I didn't mean that at all.

Paul Eggerman – eScription – CEO

No, and I think our recommendation actually covered it. It was case C, I believe.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, but it no longer applies if you're saying that in directed exchange, an intermediary can't see unencrypted.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

No, no.

Paul Eggerman – eScription – CEO

No.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

It's NHIN Direct. It's not directed exchange.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I see.

Paul Eggerman – eScription – CEO

I think we could define a directed exchange model where we explicitly carve out a trusted intermediary that has a business associate arrangement, if that's necessary, that performs the service of sending the direct message after encrypting it.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

I agree. That's the special case.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Paul Eggerman – eScription – CEO

It's either that, or we fall back to, I think we would basically have to give up on the notion of a direct exchange because PKI at the desktop level is just not feasible.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

It's probably not safe either.

Paul Eggerman – eScription – CEO

Yes, and probably not safe. Good point.

Deven McGraw - Center for Democracy & Technology – Director

So there's a special case then of a HISP or an intermediary that is doing the role of encrypting, and so we're suggesting that it leads to NHIN Direct. They're not permitted to do anything else with that data. They don't retain it. They don't reuse it. Their sole role is to route it and where that routing involves encrypting it, they may be encrypting it, which might involve some, at least theoretically, ability to see data before they wrap the encryption around it. But since that's their role, the expectation is they don't do anything else with that data. We may have to make that clear. Am I getting that right?

Paul Eggerman – eScription – CEO

Correct. Absolutely correct.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Another consideration is that we don't expect them to retain or make any reuse of that data.

Paul Eggerman – eScription – CEO

We already did that in the recommendations. We don't need to repeat that.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Does that mean, does that put that as a special case in category C or D where C is that it's access to unencrypted PHI, but we say it does not change the format or the data, or do we consider encryption to be a changing of the format?

Deven McGraw - Center for Democracy & Technology – Director

No, I wouldn't.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

In fact, in my review, I deleted the term "format" because it's too ambiguous.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, I agree.

Paul Eggerman – eScription – CEO

Wait a second. I still don't understand where we are in the agenda. Are we talking about changing the recommendations now or are we talking about the framework document?

Deven McGraw - Center for Democracy & Technology – Director

I think it's a little bit of both, Paul. We've had, I think, some what I think are some very clear desire, with respect to the pilot project that is called NHIN Direct, to say with a little bit more specificity that that kind of exchange does not need to involve access to identifiable patient information, and we might say, and particularly where the access doesn't involve something beyond encrypting. We want to take care of the special case of there is an intermediary involved, but all that entity is doing is encrypting it.

There certainly are other models of directed exchange, and I think our previous recommendation underscores those, but the gloss that I think we've put on that more clearly today is that with respect to NHIN Direct, the pilot project, we don't think that that data exposure in the middle is necessary beyond what might need to happen in order to encrypt it. But that data isn't persisted. It's not reused. It's not subject to – it won't be sold, etc. It's sort of a minimal exposure for the encryption process.

Paul Eggerman – eScription – CEO

Yes, but is that a change to our recommendation, or is that a change to the frameworks document?

Deven McGraw - Center for Democracy & Technology – Director

I think it's a clarification of the recommendation, which has always said that ONC ought to be encouraging the models that don't involve exposure to unencrypted PHI.

Paul Eggerman – eScription – CEO

All right.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

I think it could lead us to try to sort of reframe that framework, Paul, to the extent that I think it would have been easier from a policy perspective if we were able to have drawn a line that says category A is NHIN Direct, as Carol was describing, for example. The narrowest definition you could think of to say you never have exposure to PHI. Why would you do that? And you're able to draw that horizontal line across and then say everything below it is directed exchange, but it's not NHIN Direct. Now it seems like within the current framework, what we're saying is we'd want an exception, a singular exception that actually moves down almost to category C for the purposes of encryption by the intermediary, which may mean that we, just for the purposes of exposition, it may be easier a little bit later, I don't know now, I don't know if we want to do this now, to recast that so that it's a little bit cleaner to explain. Or we could keep it that way and just explain it....

Paul Eggerman – eScription – CEO

It sounds like we haven't done the recommendation. What we need to do is return to the original recommendation. In other words, I don't understand what you're saying. This is an exception to category A.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Because, well, an exception, yes. I agree. Operating the assumption that if we were kind of going, and this is where I think we were headed on this call, and this is just my interpretation of where we seem to be headed that Carol had suggested that we ought to think about a definition of NHIN Direct, which is minimalist with respect to this framework, which is to say that it's only about secure routing with no exposure to data.

Paul Eggerman – eScription – CEO

Yes, but that's not what the recommendation is about. The recommendation is about directed exchange.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Yes.

Paul Eggerman – eScription – CEO

Right?

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

True.

Deven McGraw - Center for Democracy & Technology – Director

I know, but, Paul, I'm trying to understand. We had a set – what did you think we meant when we said that ONC ought to be recommending the use of A? I think it was A and B, the models that don't expose data.

Paul Eggerman – eScription – CEO

To me, it's a simple thing. The least exposure of data and the least moving parts, the fewest intermediaries, the least risk there is, and that's the way I look at it. But it's the distinction between NHIN Direct and directed exchange. There's a general model that's in place where providers are already exchanging data, and it seems to me that the policy recommendation is around that model. If what you want to say is NHIN Direct, it's got to be limited to what's called category A. That's fine, but to me that's a separate discussion. The recommendation is not about NHIN Direct. The recommendation is about directed exchange where you go from A to B, although I did hear somebody else say that almost all of the NHIN Direct stuff assumes that there is an intermediary so at least you have category A and probably category B at least involved.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I think category A is nothing but a private network, quite frankly. I think B is really what most people on this call is thinking of as directed exchange over the Internet.

Paul Eggerman – eScription – CEO

No, I think category B might be what most people are thinking as NHIN Direct.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

Paul Eggerman – eScription – CEO

Not directed exchange, but NHIN Direct.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

NHIN Direct. I think NHIN Direct is like between B and C because it only – yes, it has access to unencrypted PHI, but only for the purpose of encrypting and routing it.

Paul Eggerman – eScription – CEO

Yes, but what we said in our discussions was once you got access, you dropped into category C.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, but....

Deven McGraw - Center for Democracy & Technology – Director

Okay, so then we are suggesting, I think people are suggesting – I'm sorry, Dixie. Go ahead.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I think what we're doing is through policy restricting it, that yes it's category C, but the only purpose is to encrypt the data.

Paul Eggerman – eScription – CEO

Yes, and....

Deven McGraw - Center for Democracy & Technology – Director

For NHIN Direct.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And the rationale behind it, just as to why the team ended up making that as part of the consensus, was that the provider who wants to participate in secure exchange of data, but has nothing other than an e-mail client at his disposal, can do so with NHIN Direct and be guaranteed that the message, once it's on the wire in the Internet, will be encrypted. But to do so, he trusts the e-mail provider, the secure messaging, NHIN direct provider, to apply his encryption keys on his behalf, and that requires that a PHI containing message go from his e-mail client up to the HISP. It goes over a secure channel. But nonetheless, the HISP actually has the unencrypted e-mail in order to apply his encryption keys on his behalf. That was the driving use case.

Paul Eggerman – eScription – CEO

I don't understand. You want to make sure we do our policy in such a way so that it works with one of your use cases?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think the goal was to say, is this approach that we've taken okay with the policy experts at ONC? So it's to bless the approach or to reject it, yes.

Paul Eggerman – eScription – CEO

I disagree that that's what we should be doing.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Okay. I've got a problem.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

It sounds like there's maybe not formally, but there's a proposed recommendation here that says that we should say that in order to be called NHIN Direct for the pilot project, you ought to be doing transactions of category B, and if you're in category C with the singular exception of encrypting data for the benefit of the provider. Is that what we're coming to as a proposed recommendation?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

That's not what Paul just said.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I don't think Paul likes that.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

No, right, I know. I'm just trying to clarify that that's what I think, Paul, it seems that a number of people are kind of headed toward here, but it sounds like you're uncomfortable with that.

Paul Eggerman – eScription – CEO

Once data is exposed, it's exposed. It doesn't matter what you're using it for in terms of exposing for category C. But if that's what people want to do, that's fine. We can change it.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

This is where I stumble over the definition of an intermediary. The only way to not expose it would be to require that everyone runs their EMR locally on a desktop PC.

Paul Eggerman – eScription – CEO

That's just not right. Why do you say that?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

If the provider, let's say an HIE in a community sets up a Web service that a provider can subscribe to.

Paul Eggerman – eScription – CEO

Wait. How does that relate to directed exchange?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I'm going to say, he sets up an e-mail, I mean, a Web client to do directed exchange. In other words, one approach is the provider's e-mail on his desktop, has his own keys in the e-mail. You know, he downloads the keys of every other provider in the country into his e-mail system, and he can encrypt before it goes onto the wire. That would qualify as A, but that's infeasible, so the fall back is either you could push a Web client out to that provider, but that means whoever is pushing the Web client out, that entity now sees unencrypted data when the provider types his message into the Web browser. He types in this patient with such and such. Boom, it's exposed to the intermediary.

Paul Eggerman – eScription – CEO

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

You can't avoid exposing to the intermediary unless you force the provider to do all the encryption on this own PC on his desktop, which is just not feasible. So category A is an impossibility. It's not impossible. It's impractical.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Category A is private networks. I think it should be not even part of this discussion. The only way it's possible, even the FTP example up in my review is exposed at every node. So I think A is not even within the realm of what we're trying to address here.

Carl Dvorak – Epic Systems – EVP

Dixie, I think A is a little bit different though. This is Carl. I think that the example that was just previously given is more of a hosting organization that does in fact decrypt it and present it to the provider in clear text, which by indirect implication has access to clear text PHI. Bucket A really does involve switches and movement of packets of encrypted information that are not necessarily open. To the extent that there's no intermediary that opens the packet, I think that really is a clear bucket of exchange that we should try to figure out how to create policy for because it is fundamentally simpler and safer than intermediaries who have got the keys to unlock the payload.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

But how the data got encrypted in the first place, even if it was a hosted service, that's PHI data that's not in the provider's – it's going to a different organization, the hosting organization.

Paul Eggerman – eScription – CEO

That's the case where you have an intermediary.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Carl is talking about category A when there's no intermediary, and I'm having a hard time coming up with an example where there is no intermediary.

Paul Eggerman – eScription – CEO

Yes, but I sent you an e-mail on this. There are tons of examples of that.

Carl Dvorak – Epic Systems – EVP

Yes.

Deven McGraw - Center for Democracy & Technology – Director

Can I interrupt here? We went round and round about this in the previous privacy and security workgroup about what constitutes an intermediary and what doesn't. I'm going to go back to a point that Carol made earlier. Whether you officially are or you're not is less important than the question of whether you have access to identifiable health information, and I thought that I heard – and we certainly have recognized models of directed exchange as distinct from what I think we're carving out for NHIN Direct, which does involve some access to identifiable information for one purpose or another. One might put into those buckets the purpose of encrypting it, and that's a minimal amount of exposure for some of us that we might be able to get comfortable with. But intermediary, not intermediary, who is one, who isn't one is not nearly as important as statements about whether you have, whether there's PHI exposure, whether any of that is needed for the NHIN Direct pilot project, which I think I was hearing at least as a model, we might be able to say as a group that we don't think it's needed with the possible exception of the limited exposure for encryption purpose, and it has to be specifically limited.

Joy Pritts – ONC – Chief Privacy Officer

Except, I would like that people on the phone call – I'm getting a little confused here because if this is a pilot project, it has a number of organizations that have volunteered to participate in the project, and what it seems to me is that you're saying that either they can't participate or they can't follow their potential use cases from what Wes was saying. Is that what the intent is here?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

No. I think where this is going is to say that for the NHIN Direct approach from a technical perspective, what we are saying is the approach should not require technically the exposure of data or metadata in order to get the point A to point B direct sending of a message. And I agree that the encryption service is potentially an exception to that, but what I think is important to understand in this discussion, which isn't clear to me is completely understood is that there are multiple ways to accomplish point-to-point communication. Some of those ways, by their very technical nature, require the exposure of PHI or metadata.

Joy Pritts – ONC – Chief Privacy Officer

Carol, I'm going to be really blunt about this because I know I can be with you.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Yes.

Joy Pritts – ONC – Chief Privacy Officer

It seems to me like what you're doing is rearguing the two technical means that the group agreed to last Friday that they were going to follow in NHIN Direct care. Is that right?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

No.

Joy Pritts – ONC – Chief Privacy Officer

No. This isn't about STMP?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

No, it has nothing to do with it.

Joy Pritts – ONC – Chief Privacy Officer

It isn't about IAP?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

This is about any method of point-to-point exchange that is endorsed that requires information to be exposed in the middle. I don't care what it is, right? There is a way to accomplish point-to-point exchange that does not require the exposure of the payload in the middle, and there's a way to do it that does require exposure of the payload in the middle.

Joy Pritts – ONC – Chief Privacy Officer

Why don't we phrase it that way, which is I think is fairly close to what the recommendations were, and I don't mean to be putting words in people's mouths, but I think this is what I'm hearing, which is that in directed exchange, there should not be exposure of the payload.

Paul Eggerman – eScription – CEO

You mean in NHIN Direct?

Joy Pritts – ONC – Chief Privacy Officer

No. Let's just start with directed exchange as a policy. Is that what you're saying, Carol, as a policy, general policy?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Yes.

Paul Eggerman – eScription – CEO

Yes, but, Joy, we can't say that as directed exchange because there are organizations like SureScripts that expose what you call the payload and reformat it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

But they aren't directed exchange. That's not what we agreed on.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

That's not directed exchange.

Paul Eggerman – eScription – CEO

What are they?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

They're more like an HIE. We talked about that there are many models of exchange, and we're trying to focus on the very minimalist sending information from point A to point B. That's not SureScripts is more an HIE.

Joy Pritts – ONC – Chief Privacy Officer

This goes more to the four models that you used to set up this discussion to begin with, which I think actually are somewhat helpful because without calling it, there seems to be some issue here about whether you call this directed exchange or not, but just not use the term and describe what it's intended to do. So if somebody is sending information, just like you did originally, I think you had categories of they're sending information without directly accessing PHI. They're sending information, and they are directly accessing it, but you had said here. Perhaps accessing it just to encrypt it would be a different – raise different concerns. Then your next one, I think I'm hearing you say, is that if you're sending information and somebody, a third party in the middle or whatever you want to call them is not only accessing protected health information, but is also somehow manipulating it, that's another category that raises different concerns without calling it necessarily directed exchange or what. I mean, I guess we're going to segue into the other conversations, but if that's where we're headed, I think that's where we're headed.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Let me kind of do a variant of what David suggested that I think Paul would be okay with. If I were a provider and I logged into a Web site, and I created a record or e-mail message to make it really easy. I created an e-mail message to another provider on that Web site, and I pressed the button that said encrypt message and send to Dr. B, and I hit send. Now technically that software as a service provider is an intermediary, and technically that information that they put in the e-mail message would be exposed because that software and service provider would have been encrypting it, right? That's who encrypted it. But I think that Paul would be – I think, Paul, you would be comfortable with that more than the scenario that David explained where somebody sends it to the service provider. Am I right?

Paul Egerman – eScription – CEO

I don't understand what you mean by whether or not I'd be comfortable with it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Would you consider that a direct exchange?

Paul Egerman – eScription – CEO

It's hard for me to know because just because it's software as a service does not necessarily mean it's an intermediary.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

It is. Yes, it is. You're going to somebody else's.

Paul Egerman – eScription – CEO

No. An intermediary means that it's somebody between the EMR, the computer system of the sender and the computer system of the receiver. That's what an intermediary is. Now if all you do is sign on using the Web browser, you're still just using a service to sign onto your own EMR, so that function, in my opinion, is not a directed exchange function.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Actually, I think we're having sort of different conceptions of what "the system" is here.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Point A.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

We've been thinking of the source or the destination of the message as possibly being a system, but often being someone using software that is either e-mail software or is not much more sophisticated than e-mail software.

Paul Eggerman – eScription – CEO

I don't know. E-mail is an interesting issue, but to me this is all a discussion about directed exchange, which is literally between two computers.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

No, that's not what....

Paul Eggerman – eScription – CEO

A patient is admitted to the hospital....

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

If in fact that is where you are taking the definition of directed exchange, then I would say that is fine. It just doesn't provide a lot of help to the NHIN Direct project because the NHIN Direct project has many user stories that are different than that. Frankly, that's what NHIN Exchange is, is computer-to-computer transfer of information.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

It's not computer-to-computer. It's legal entity to legal entity, so I guess where I would disagree, Dixie, with your framing of that being an intermediary is I think that's an overly broad definition of intermediary for the purposes that we are working here because I would consider that, and this is where I argue with Paul that the configuration of your electronic health record shouldn't matter in this conversation.

Paul Eggerman – eScription – CEO

Right.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

And so if I have a software as a service as my electronic health record, that is just the true enough, my data is going to them or is entered in their system, but that is a company that is just manipulating and managing and documenting and providing me with a vehicle for me, myself as an organization, to better manage my own data. But it is not, explicitly not exposing it to anyone else under the terms of the contract I have with them. As soon as they then, on my behalf, send it to someone else, if they do it directly, then that's our category A, meaning they send it to another EHR directly, let's say. If they do it through some type of HISP or HIO, then that's the intermediary category that I think Paul was referring to. I would agree with that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

This is David. I think, Micky, your description of how the EMR, remote hosted EMR would work is exactly the same way and a HISP would work in NHIN Direct. It is a service provided to that provider under contract to package up, encrypt, and send the message exactly the same way the EMR is the service provided under contract to that provider to manage his patient's record.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Except....

Paul Eggerman – eScription – CEO

Let me just break in a minute here. We're talking about a fairly interesting and low-level technical issue, which is like service as a service and EMRs, and I just want to understand where are we on the agenda. Deven, what is the question that we are trying to answer here?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Transparency.

Deven McGraw - Center for Democracy & Technology – Director

No. I think we've moved well beyond the transparency.

Paul Egerman – eScription – CEO

Yes, so I'd like to get ourselves refocused on what is the question that we're trying to answer because this is an interesting discussion, but I'm afraid we could take up another three weeks on some of these issues. Are we still on transparency?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Paul, there comes a point when managing the agenda actually becomes counterproductive.

Paul Egerman – eScription – CEO

I don't think so.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

And I think you have reached it.

Deven McGraw - Center for Democracy & Technology – Director

Here is where I think we are. I think we did depart from talking about this framework document, but I actually think – I thought we were headed to a goal, which is to say, we recognize, as we did in our document, that when you talk about directed exchange where there is an entity in the middle that might be facilitating that, there could be varying levels of exposure to data, and that the models that expose to data, and that the models that expose the least amount of data are preferred. And, in fact, what I certainly have been hearing on this call is that with respect to the pilot project known as NHIN Direct, we're not sure that any – we don't think any exposure is necessary beyond this model that enables the intermediary to be exposed to data just merely to encrypt it for no other reason, no other use beyond that in order to avoid a problem of not being able to scale PKI for direct exchange. Again, I don't think that's at all inconsistent with the directed models, but it puts a gloss on it with respect to the NHIN Direct project. Yes, that was straying beyond the transparency comment, but I still thought the discussion was very helpful to the set of recommendations on the table.

Paul Egerman – eScription – CEO

Is the question we're trying to answer this? Let me see if I can phrase the question. The question is, does this group want to put a constraint on NHIN Direct that says something about the level of PHI exposure that is going to be allowed? Is that the question that we're trying to answer?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I think that you hit the nail on the head, Paul.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I think when you have that movement of PHI and exposure of PHI, even though it is for encryption, it raises the bar that whoever is doing the encryption has to meet perhaps a higher level of trust for the public to be able to accept that. And there needs to be, built within that, if you're doing that little exception, then you have to have the business agreements in place. You have to have all the safe, a degree of safeguard because they are exposed. The PHI is exposed.

Paul Egerman – eScription – CEO

The questions that we're trying to answer is do we want to put any restrictions on the NHIN Direct? Is it NHIN Direct or is it on NHIN Direct pilot related to exposure of PHI?

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Paul Egerman – eScription – CEO

Is that the question we're trying to answer?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Paul Egerman – eScription – CEO

Does anybody have a proposed answer to that question?

Deven McGraw - Center for Democracy & Technology – Director

Yes. I'll attempt to articulate it, and I'm sure folks will correct me. I'm gleaning this from the conversations that we've had on the call, which is to say that for the pilot known as NHIN Direct, I feel like it's the artist formerly known as Prince, you know, there isn't a need to expose data. This is exposed PHI to, number one, there's either no intermediary involved, depending on how you define intermediary, or it's that level B, which is there isn't any exposure. That's one set of recommendations. Then we could move to a second sort of case where we recognize that one of the models that the technical team is considering would provide for such a minimal amount of exposure in order to encrypt the message before sending it on. That could be permissible only if it was – that's permissible as a sort of best practice model B, only if it's that exposure is limited to merely encrypting the data.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

This is David. That sounds good to me. I think there are some other areas where the NHIN Direct team has sought guidance as well. But I think you covered it pretty well with those two, the exposure part.

Paul Egerman – eScription – CEO

If we're in agreement on that, let's say that's our recommendation, and let's move on.

Joy Pritts – ONC – Chief Privacy Officer

Can you read back the recommendation right now so that we know we have agreement before we get off the phone?

Gayle Harrell – Florida – Former State Legislator

And you're saying that there will be no other constraints, that there's no requirement?

Deven McGraw - Center for Democracy & Technology – Director

No. What I'm referring to is that we have a set of recommendations that go to directed exchange with some models that we've described there. And I'm not attempting to change those. I'm adding a gloss on those with respect to the NHIN Direct project that that's model A or B, which is non-exposure to PHI at all to the intermediary. Then secondarily, we're making, we call it an exception to the exception.

We understand that the technical team is pursuing an encryption model whereby there is an intermediary in the model. They do have some exposure to data, but it's minimally for the purpose of encrypting the data before passing it on to the other provider. There's no data retention. There's no other use of that data. The data is not changed. It's not manipulated. It's merely for the purpose of encryption, and for those limited reasons, for the NHIN Direct project, we could understand why there might need to be exposure to data, which would otherwise be not necessary for the purpose of NHIN Direct.

Now that doesn't, I mean, I'd like to continue. We have another 45 minutes. I'd like to continue to talk about this framework document and see if we can tick off a few more. We got comfortable with some pieces of transparency so that patients are more aware that we're moving to a new environment with electronic medical records and electronic health information exchange, the sort of first two prongs, but not articulated in terms of guidance that HHS needs to take some steps to make this – to insure that this gets made transparent to patients. Then I'd like to move to some of the other prongs of this framework and see how many we can tick off. Does that answer your question, Gayle?

Gayle Harrell – Florida – Former State Legislator

The only thing I want to clarify is that when you do move to that area where you have the PHI exposed moving it so it will be encrypted, that at that level there are some safeguards. Are we saying that that is just as if it were encrypted, or it's acceptable to have it unencrypted and move it to encrypted, and that there will be no additional requirements, no safeguards required?

Deven McGraw - Center for Democracy & Technology – Director

No. That's a good point, Gayle. I think the way that I would articulate that is certainly because we're talking about the sort of what's the container, to use Micky's term, for NHIN Direct, I would say that that intermediary or HISP or whatever you call it in the middle for which there's some exposure to PHI, it has to be strictly limited to just encryption and no persistence of data, no retention, no further use, no access beyond what's necessary to encrypt it.

M

And no transformation of data.

Deven McGraw - Center for Democracy & Technology – Director

And no transformation, no changes, I mean, that's the sort of acceptable level of constraints around something that otherwise would be in our directed exchange model C or D.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I hate to be technical, but with respect to Micky's use of the word transformation, there was a compromise reached between the proponents of the SMTP model and the XDR model to allow a sort of rearrangement of the data such that XDR users would be satisfied with it, so it's not changing anything clinically, but it is rearranging.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I don't support that.

Deven McGraw - Center for Democracy & Technology – Director

Now we have too many exceptions to the exception.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

Paul Eggerman – eScription – CEO

Yes. Let's try to understand, what are we trying to accomplish? I thought we had a question, and I thought we had an answer to it.

Carl Dvorak – Epic Systems – EVP

I'm wondering Paul, if we need that second part about the encryption or not encryption on an outside party. It seems that that opens up a can of worms, and I don't think you really need to do a third party encryption because it would still be within your walls ... I'm wondering if you could exclude that ... for simplicity and still have a policy.

Paul Eggerman – eScription – CEO

I'm trying to understand what you said. Could you or somebody sort of say the answer to the question with the encryption part out of it? Do you understand what I'm asking for?

Carl Dvorak – Epic Systems – EVP

Yes. I was trying to remember how Deven phrased it though. Deven, would you be able to phrase it without the encryption part, the first part?

Deven McGraw - Center for Democracy & Technology – Director

Carl, I can't say for sure that I know what you're talking about – that I understood your point, which is to say, you know, what I said, what I thought I was hearing on this call, and maybe folks were just not piping in, which is clearly not a wise thing to do, but is with respect to a subset of directed exchange called NHIN Direct. We wanted to create a policy space that was very clear that there ought to be no access to identifiable information by anyone serving as an intermediary in that transaction. So it's essentially in a directed exchange model A or B.

Carl Dvorak – Epic Systems – EVP

I would agree.

Deven McGraw - Center for Democracy & Technology – Director

You could end the sentence there, and then I heard that because end-to-end encryption, PKI infrastructure is not scaleable for multiple providers, as they would like NHIN Direct to be. There is a request on the table for an exception for an intermediary that merely encrypts and has no other access to data beyond what's necessary to do that, and doesn't persist it, doesn't reuse it, doesn't do anything beyond that. Then you wanted me to articulate it in the context of something else, and that I can't do.

Carl Dvorak – Epic Systems – EVP

My point was that I'm not sure you need that secondary portion of an intermediary that encrypts to decrypts for you.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

This is David. You do need it for the current consensus proposal.

Carl Dvorak – Epic Systems – EVP

Let's take the current NHIN Direct construct aside for a second. I think it would be beneficial to define a vanilla direct exchange model and see if the NHIN Direct folks could adapt to something. I think policy informs implementation and implementation sometimes needs to inform policy. So I think we may want to go back to the NHIN Direct folks can understand if the world were simplified to say there were no intermediaries with access to PHI, is that a practical implementation objective for them to put in place?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Let's assume for now that we've spent roughly six weeks having that discussion in NHIN Direct. What's the right forum for getting that discussion closed with this committee?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Because we debated exactly that question for at least six weeks.

Joy Pritts – ONC – Chief Privacy Officer

And what was your conclusion?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

That if you want to reach providers that don't have current EMRs, you need to allow for a trusted intermediary to manipulate this data for them to encrypt it.

Joy Pritts – ONC – Chief Privacy Officer

Why was that?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

So that you could use an ordinary e-mail client or a simple Web browser client on the desktop of those providers who don't have EMRs.

Joy Pritts – ONC – Chief Privacy Officer

And what happens if you don't have the third party doing the encryption?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Then all providers would be required to manage their own PKI to do encryption on the desktop themselves, which was, we all agreed was infeasible.

Carl Dvorak – Epic Systems – EVP

Let me back up one....

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

It's an approach that has failed already.

Carl Dvorak – Epic Systems – EVP

No. Let me back up a second, Wes, because I'm not saying you couldn't take that approach. I think what we're saying is that you would just have to continue to define policies that were appropriate for that approach. I think we may want to define a direct exchange model that does not allow the intermediary in any case to open the package, and then continue the work, which we'll need to anyway for HIEs in general to define the next step, which is what happens if they begin to open the packet and can see PHI material. I think a good, concrete, doable first step that would be practically useful is directed exchange where nobody opens the envelope.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Where would you find? Is this something you say is going on now? Is that right?

Carl Dvorak – Epic Systems – EVP

Yes.

Paul Eggerman – eScription – CEO

It is going on, which it's interesting because everybody has in their head like a different mental model as to how this whole thing is currently working and how it should be working. But what Carl just described is going on, and it's going on in lots and lots of environments.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

What would be an example? Help me understand.

Paul Eggerman – eScription – CEO

Epic has this thing called Care Everywhere, where....

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

So EHR vendors are communicating to EHR vendors without having to have unencrypted data. That's understood.

Paul Eggerman – eScription – CEO

No....

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

...the other case that....

Paul Eggerman – eScription – CEO

No. First of all, it's not EHR vendors. It's customers of the EHR vendors. They are the ones who are communicating to providers.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Customers are using the EHR vendors as their intermediaries.

Paul Eggerman – eScription – CEO

No, they aren't.

Carl Dvorak – Epic Systems – EVP

No.

Paul Eggerman – eScription – CEO

The healthcare providers are communicating back and forth, but let's go back to basics.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Wait. No, I want to understand. You're saying that without using the Epic system, Epic customers are communicating to other physicians or to other Epic customers?

Paul Eggerman – eScription – CEO

Other Epic customers.

Carl Dvorak – Epic Systems – EVP

And....

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

So are they using the facilities of the EMR or not?

Paul Eggerman – eScription – CEO

They're not passing their data through Madison, Wisconsin. They're using software that Epic may have written, but everybody uses software written by somebody. But it's....

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Whenever anybody uses software at both ends written by the same vendor, we have a very closed arrangement. I'm not arguing that this is not going on. I'm arguing that it's not what we're trying to do.

Paul Eggerman – eScription – CEO

It is going on. Let's go back to basics.

Carl Dvorak – Epic Systems – EVP

Let me....

Paul Eggerman – eScription – CEO

We have two concepts here. We have directed exchange, which is the general case. We have NHIN Direct, which is the more specific case, which is the case that people want to constrain. We have a question on the table as it were, which is, what constraints does this group want to place on NHIN Direct? The proposal is basically almost nothing should be unencrypted except when necessary to do encryption. That's the proposal.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I would say that there was a thought or a request to consider where there were different requirements on an intermediary that provided encryption rather than one that didn't, such as having to have a business associate agreement or something like that, but fundamentally ... right level of distinction. Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Deven had a very specific proposal that we had all accepted. I'm not sure why that....

Deven McGraw - Center for Democracy & Technology – Director

Well....

Paul Eggerman – eScription – CEO

Yes. I want to go....

Deven McGraw - Center for Democracy & Technology – Director

I'm not sure that we all had, but....

Paul Eggerman – eScription – CEO

Yes, I think Carl did not accept it. Is that correct?

Joy Pritts – ONC – Chief Privacy Officer

No. Carl – I'm going to jump in and speak for Carl, challenge Carl there. Carl, I think, is asking that a slightly different scenario be considered. Is that right, Carl?

Carl Dvorak – Epic Systems – EVP

My suggestion, and I didn't mean to create this much swirl on it, was that first off I think NHIN Direct actually will transcend many different types of exchanges all the way from full HIE interaction down to a direct provider-to-provider exchange. So I think the question might be a little bit reversed. My thought to Deven's comment was you could stick with the part A of her statement, and you could drop the part about opening the packet for purposes of encryption because I think as soon as you get anybody who has got the open package, you have to define rules for what they might and might not do with it.

I was just suggesting that we take this in bite-sized steps, which is to say a directed exchange that does not open the packet may exist under this set of rules. If you open the packet, then there's another set of rules, and we may want to graduate those set of rules depending on what limitations we impose when the packet is open. But I think we have to take it in bite-sized pieces, and one clear bite sized piece that does happen, and it's not just an Epic-to-Epic thing. I want to be real careful with that. We do that with Meditech, and I know that other providers do very similar things with the same mechanism. It does not go through an intermediary, so it's not an Epic thing anyway. But my suggestion was, let's take it in steps, a directed exchange where no one is allowed to see the content of the packet, and then work to graduate that up to scale where people can open the packet and start to do things with it and figure out what additional policies layer on with that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

But we are at the point where we need to take that next step. I mean, we chewed up the first bite, I think, which is a good starting point, and are now wrestling with how to rope in the 600,000 physicians that don't have access to the technologies to do step one.

Carl Dvorak – Epic Systems – EVP

I'm not sure we've got agreement on step one, so it might be good to actually state the agreement on step one and then move on to step two and define how much PHI is exposed in step two and what policies apply to that, and then move on to the more sophisticated steps with full blown HIE.

Deven McGraw - Center for Democracy & Technology – Director

What we have had on the table for the last several calls now and that is the document that Paul began discussing in the beginning of the call is a set of directed exchange models that run the gamut from the A model, which is direct and absolutely no exposure to unencrypted PHI, and I don't have them in front of me. B also involves exposure. Then you sort of go up the chain to more exposure, either because there's a change in the data or there's manipulation of the data, etc. Clearly we have always said all along, and the document has said all along that the model that involves no exposure raises the least amount of privacy risk. Those should be best practices for simple, directed exchange. We have said that all along. There is nothing different about that.

I think what we're grappling with here is whether some particular – whether we want to create a space for NHIN Direct that can find it clearly to the models that don't expose data, and I think folks are – what I heard largely from the group was that people did think that was possible. However, the technical team has let us know that they are considering a model that would involve some minimal exposure. What's less clear to me is whether there's anybody comfortable with saying that if there's this container called NHIN Direct where there's no exposure normally, we might make an exception in this case. I'm not sure that the group, that there's consensus around that piece. And maybe we're not able to – maybe we can discuss that in a little bit more detail, but the recommendation model that we have been discussing for many weeks now is one where we have endorsed greater sets of policy requirements for greater exposure to data.

We have said all along that the recommended course is no exposure at all model, and now if we want to sort of create that horizontal line that Micky was talking about for NHIN Direct and what does that mean, clearly the least amount of exposure possible is the one that we want. To the extent that there might not need to be some exceptions to that, we should probably discuss them because that's a viable model that's on the table. But I'd prefer to be doing it in a way that considers as the threshold that the least amount of exposure possible is always the most desirable. If that data never gets collected in the first place, then I don't have to worry about what happens to it down the road. However, if we can't do the simple point-to-point exchange with encryption that we want in that model, I think it's good for us to talk about it, recognizing that there are some models that fit under A.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

This is David. I think that's well posed set of questions. I would argue that the model where the service provider, the NHIN Direct service provider performs the encryption on behalf of the physician so that he doesn't have to do it on his own desktop is exactly analogous literally to a remote hosted EHR.

Paul Eggerman – eScription – CEO

No, it isn't.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think it is.

Paul Eggerman – eScription – CEO

I disagree.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

It's a remote service that's providing – that you have a business associate arrangement with that provides the data manipulation of PHI data just like a remote hosted EHR does.

Paul Eggerman – eScription – CEO

I disagree, David, but it's not important for this discussion. It's an interesting point, but you have to understand, Deven and I need to report something on Friday. We need to stay focused on what it is we're trying to resolve. Whether or not....

David McCallie – Cerner Corporation – Vice President of Medical Informatics

...if it's off subject, I was trying to justify Deven's original proposal and say that it's not a stretch outside of accepted and common policy in use today. That was the reason for bringing it up was just to say that her original proposal was not a stretch. It is common practice today.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Can I just jump in here and try to clarify something?

Deven McGraw - Center for Democracy & Technology – Director

Yes. Go ahead, Carol.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

I think we're ... a little bit two things. The first is, Deven, the first point you made about NHIN Direct. I think what we're saying at the base layer is really not a statement about intermediaries. It is a statement about the requirement for the technical approach to simple exchange, point-to-point exchange. And what we're saying is that the requirement should not require the exposure of PHI. In other words, there are ways to accomplish point-to-point exchange that by definition will expose PHI in the middle, either in data

or metadata. What we're saying is for the simplest case, that exposure is not necessary. It's not so much a statement about intermediaries.

What we further said is to start to think about where intermediaries may be required. And to the extent that simple exchange may require an intermediary to perform an encryption service, it's a valid point. But for me, it begins to raise the sort of next layer of work, which is, what are our policies for intermediaries as opposed to going back to the question of policy guidance for the direct exchange, for the technical specifications of direct exchange. I hope that's clarifying.

Deven McGraw - Center for Democracy & Technology – Director

I think it is a little bit. I think the clearest picture that I'm getting from this call is a very clear indication that when you're talking about direct exchange, models that do not expose data to an intermediary are certainly preferred.

Joy Pritts – ONC – Chief Privacy Officer

Deven, can I jump in here a minute?

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Joy Pritts – ONC – Chief Privacy Officer

I want to ask Carl if there was something in addition, additional protections that you had in mind or thought were necessary in the base model where there was no intermediary.

Carl Dvorak – Epic Systems – EVP

I think guidelines around what does it mean to do proper encryption and things like that aside, I don't think, provided you have patient consent, and you have the certificates that help you understand it's truly the right endpoint that you're talking to or hearing from, I think you're okay.

Joy Pritts – ONC – Chief Privacy Officer

Okay.

Carl Dvorak – Epic Systems – EVP

Then as you go to that next layer, it's okay. It just means we have to define rules around that layer because it's one thing on a policy call today it's included, but someone is going to have to write down the rules of what that means, and I think that's going to become much more expansive than we imagine right now.

Joy Pritts – ONC – Chief Privacy Officer

Thank you. Sorry, Deven, but I wanted to nail that at least layer one down.

Deven McGraw - Center for Democracy & Technology – Director

Okay.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Carl, this is David. Is layer one possible without an EMR or must you have an EMR?

Carl Dvorak – Epic Systems – EVP

I don't know that you necessarily have to have an EMR. You simply have to be in possession of decrypt technology and an appropriate certificate, so it could facilitate being an endpoint without an EHR present.

Again, I think, David, it simply means that to go to that next step, you just have to write down what policies apply to that next step. I'm not arguing one way or another on the appropriateness of that step. I think it's an okay thing to do, and it's nice to reach out to those folks who will not have an EMR in time.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think that's....

Carl Dvorak – Epic Systems – EVP

...policy there.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think that's what NHIN Direct is trying to do.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I think we're just at a really important point here, which is that it's easy when there is a healthcare organization that operates the technology because they encrypt their own stuff. It's easy when there is a vendor that has the business associate agreement with the healthcare organization, such as a remotely hosted EHR vendor, but it doesn't have to provide all of the EHR services to fit into this category because we're hoping that the policy approach considers an entity with a business associate agreement as approximately the same as the entity itself, as the covered entity itself because that's how a lot of EHRs work now. Then there is the – and if in fact we were to say those are the only two cases are an intermediary that has no access to the protected health information except as an opaque stream of encrypted bits, and that an intermediary that has a business associate agreement, I think that would be a really good distinction to make and pretty helpful.

Paul Eggerman – eScription – CEO

That's what we tried to do in the recommendations, but—

W

Yes.

Paul Eggerman – eScription – CEO

I know, Wes, you don't like it when I talk about the agenda. I'm still confused. Where are we right now?

Deven McGraw - Center for Democracy & Technology – Director

Here's where I think we are, my attempt to clarify it here. I think we are, in terms of directed exchange models, we have four. We said very clearly that the greater access that an intermediary has to data raises the level of risk, requires some additional policy. We need to and want to think about those.

Then we moved on to considering whether there was a horizontal line that we would draw and make a recommendation to ONC that from a policy perspective with respect to the pilot project called NHIN Direct, that that ought to be a model that exposes no data in the transport, and people seem to be very comfortable with that. And where there is some disagreement is whether there ought to be some blessing of the use case model whereby there is an intermediary that has access to data, but it's for a very limited purpose of encryption, and that in order to bless that, I guess I would go a step further to say that there would need to be very clear limitations on that intermediary's access to data, and that it is for that encryption purpose only, but there is some disagreement among the workgroup as to whether that model is needed, but it is certainly one that is being considered today by the technical team.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Deven, can I ask a question about what you said?

Paul Eggerman – eScription – CEO

Just a second.

Deven McGraw - Center for Democracy & Technology – Director

You can ask a question. I'm not sure I'll be able to answer it. But I'm trying to keep this at a policy level without diving down too much into model choosing.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I understand. I'm just suggesting that we recast the question to a level of policy that applies when the intermediary does have a business associate agreement and when there is an intermediary that doesn't have a business associate agreement, and not talk about exceptions to the intermediaries. It's just make those two pretty clear and well understood conceptual....

Deven McGraw - Center for Democracy & Technology – Director

Yes, except that it's not a terribly helpful distinction, Wes, in my view because the business associate agreement is just a vehicle or a tool for enforcing policy. And I think we need to, at a first flush, get to the issue of the policies that ought to apply when intermediaries are involved, and they have access to data.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I understand that.

Deven McGraw - Center for Democracy & Technology – Director

They have any access, yes.

Paul Eggerman – eScription – CEO

Let's return to the question then that Deven is asking. We've got a partial answer, and the partial answer, the part that's unresolved is whether or not this is sort of like carve out or exception that allows an intermediary to encrypt unencrypted data as part of NHIN Direct, not as part of directed exchange, but part of NHIN Direct.

Deven McGraw - Center for Democracy & Technology – Director

Right. That's right.

Paul Eggerman – eScription – CEO

That's the issue on the table. Who wants to say they disagree with that?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

This is Dixie. I have – here's how I feel about it. I think if a third party, an intermediary, which one you want to call them, if an intermediary provides to the user a service that enabled that user to encrypt data and send it to provider B, I'm perfectly fine about that. I'm a little weary about the notion of the provider, the sender sending a packet of information, an e-mail, whatever, a record, whatever to an intermediary and then that intermediary doing the encrypting and applying the digital signature. I think it certainly is technical feasible for an intermediary to provide that digital signature and encryption as a service to the user, and I'm happy with that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Wait a second. I'm confused. Are you saying that you are in favor of what I'll call the carve out, the allowance, or you're not in favor of it, or you're saying you're only in favor if there's a further refinement of it?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

B, I'm not in favor of it as an explicit carve out without some constraints. I think the encryption should be in the control of the sender, not just – I object to a handoff of an entire block of data or documents. Okay. I'm a provider. I have a document. I object to just handing off that document to a third party and saying, okay. Have at it. Apply my signature to it. Encrypt it for me. Have at it.

If, on the other hand, that intermediary allows me, as a sender, to – it provides a service to me such that I can go to their Web site, and I can type out, I mean, we all do this. You go to a Web site. I type out an e-mail. I attach my document, and then they encrypt it and send it on to the end. I'm perfectly happy with that.

Paul Eggerman – eScription – CEO

Okay, so....

Deven McGraw - Center for Democracy & Technology – Director

Yes. I'm having a little bit of trouble distinguishing it too.

Paul Eggerman – eScription – CEO

I'm sorry. Go ahead, Deven.

Deven McGraw - Center for Democracy & Technology – Director

No, Paul. I don't know if you saw it. I'm having a little trouble, Dixie, understanding what's the distinction. Is it that the provider A clearly directs the intermediary to apply the encryption?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

No.

Paul Eggerman – eScription – CEO

Let me make a suggestion to everybody on this. People may not like this, but we've already said as a policy group that the encryption is good. Unencryption is bad if that's what we prefer to do. But I'm just concerned that we're starting to get too far into the technical details as to what the pilot project is going to do. Haven't we given them enough guidance by saying what we said? In other words, it seems to me at some point we're getting to a point where what I don't want to do is I don't want to find out what the specific proposals are going to be done tomorrow, and for us to be like saying, yes, this is fine as long as you do this. Is the general guide that encryption is good? This other thing is less good. Is that a good enough response?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

It's a matter of control. It's a matter of control. I don't think, from a policy perspective, and I apologize. I'm trying very hard. I don't think from a policy perspective it should be acceptable to allow somebody else, a third party to apply digital signature to encrypt and have at my information. If that person, if that third party on the other hand gives me a service, allows me to go to a Web site, log in, put together my information, put my information in there, and push a button that says encrypt and apply my digital signature and let go. That gives me control of it, even though technically it's exposed on their Web site. I have control. That's the difference. I as a sender have control.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I'm having a little trouble understanding this distinction. What I understand is that – is it the act of pushing the button that says encrypt that makes the difference to you?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

The person, yes. Well, yes, and the service provider doesn't technically, well, for example, let me go back.

Paul Eggerman – eScription – CEO

Let me see if there's another way to solve this issue, which is, in my mind, directed exchange and NHIN Direct should be focused on communication between entities, and I'm worried that we're talking about communication between an individual and an entity, and I'm saying maybe that's a totally different discussion. The NHIN Direct ought to be just talking about communication between entities and even communication between computers. That's where our biggest challenge is right now anyway, and so if we can stream it that way, does that solve your problem, Dixie?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

No. NHIN Direct is about exchanges between providers, people.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, it's very individual oriented. Computers is allowed, but....

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

That's what NHIN Exchange is about is about....

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

No, NHIN Direct.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

No. What Paul is saying NHIN Direct ought to be about is what NHIN Exchange is about.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I agree.

Paul Eggerman – eScription – CEO

Yes, but it seems like people are....

W

...NHIN Direct....

Deven McGraw - Center for Democracy & Technology – Director

Paul, go ahead. Paul is cochair. I'm going to....

Paul Eggerman – eScription – CEO

Well, it just seems like we're talking about an interesting case, which is, if I'm getting this right, it's a case where somebody doesn't have an EMR, which is what I was heading toward. And that's not, I mean, what we're all about is getting people to buy EMRs, first of all.

Deven McGraw - Center for Democracy & Technology – Director

Well, no....

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

So then it should go down that the committee chairs don't agree with the purpose of NHIN Direct.

Deven McGraw - Center for Democracy & Technology – Director

No, Wes. That's not what we're saying.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Well, that's what it sounds like.

Deven McGraw - Center for Democracy & Technology – Director

No, I don't think that's what we're saying. There's a modular certification approach that you guys approved that doesn't require people to necessarily buy a full blown EMR if they don't want to. There are sort of a number of models on the table. Some of them will be full blown EMRs. Some of them will not be. Ideally, directed exchange ought to have a set of policies involved that accommodate all of those models, so I don't think that's where we're going.

Paul Eggerman – eScription – CEO

Yes, but where I'm going is, if I'm hearing it right, a lot of what the NHIN Direct people are worried about is a physician who has absolutely no EMR, but somehow still wants to communicate with NHIN Direct.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Right, that's right.

Paul Eggerman – eScription – CEO

And that's an interesting issue, but that's not the model that I think should be driving what we're trying to get done. We've got a lot of work here to get done.

Deven McGraw - Center for Democracy & Technology – Director

Yes, but, Paul....

Paul Eggerman – eScription – CEO

And that's ... exodic case. That's not meaningful use.

Deven McGraw - Center for Democracy & Technology – Director

No, that's not....

David McCallie – Cerner Corporation – Vice President of Medical Informatics

No, it's the most common case of all is the vast majority of physicians don't have and won't have EMRs, and yet they need to receive secure communication from those physicians who are seeking meaningful use.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

And that is the intent NHIN Direct.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes.

Deven McGraw - Center for Democracy & Technology – Director

And we don't necessarily – that's exactly right, and that feels like form over function discussion to me. Like none of the models we put on that original set of recommendations said that thall shalt have an EHR to do all of this. We never made that presumption. It was about message handling. It does not necessarily require an EMR, and I think that's exactly where we should stay. In terms of handling message, again, we have always said we are absolutely most comfortable with the models that don't expose data.

What I've also heard a level of comfort with is that if you're going to draw a horizontal line, and we'd like to on NHIN Direct, that it ought to be a model that doesn't expose data. The piece that we're struggling with is whether if there is an entity in the middle performing the encryption function, if that's an exposure of data that is beyond where the comfort zone is for some folks, even if it's got some pretty strong constraints around it. You know, their access to data is limited merely to encrypting it at the provider's direction and passing it along.

Paul Eggerman – eScription – CEO

Here, Deven, is a way to solve this now that I understand what people are trying to do. Suppose we said this very simple thing that the policy recommendation for NHIN Direct is all of the communications have to be encrypted. There's no unencrypted unless there is a use case where there is no alternative.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

No.

Deven McGraw - Center for Democracy & Technology – Director

Yes, I'm not sure I understood that.

Paul Eggerman – eScription – CEO

Well, if there's no alternative because the individuals have to do something on a Web site, then let the individuals do it. I thought that was a solution.

Joy Pritts – ONC – Chief Privacy Officer

No.

Paul Eggerman – eScription – CEO

That does not work?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

No.

Joy Pritts – ONC – Chief Privacy Officer

No.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Could I...?

Deven McGraw - Center for Democracy & Technology – Director

It feels a little unconstrained to me, as you've articulated it, but maybe I didn't fully understand it. Dixie, do you want to give it a go?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes. I wanted to further clarify to Wes' – the difference in my mind if a provider, and if a provider goes to a Web site, logs in, puts in information, and encrypts, you know, says send this encrypted and digitally signed. That Web site will require that that individual provides some password or something to decrypt their private key. In the other scenario, that individual would not have that control. So the whole topic of individual control over digitally signing something is important to me. So I think that the user that's sending it needs to have that control and not just be passing off a block of data and saying go have at it.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

That's what I've been trying to focus on what service you can buy from what category of vendor, and I've tried to use, there's a business associate agreement as a way of categorizing the vendor. But I'm not – I'm a little, well, I understand your distinction.

Deven McGraw - Center for Democracy & Technology – Director

Yes. I think I understand Dixie's distinction. And it is the case, Wes, that a business associate agreement is going to be required for any model where there's some PHI exposed in the transition. I mean, that's already law. To me, what's more important is that the functionality of that intermediary is, if there's going to be some carve out that we would bless, it would be extremely limited to that intermediary providing an encryption and application of digital signature function at the specific request of the provider with no other access to that data for any purpose whatsoever.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

And no access to their private key.

Deven McGraw - Center for Democracy & Technology – Director

Yes. I'm not a PKI expert, so....

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

You don't want to give a third party access to your secret key.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Dixie, I don't want to do it here, but we need to go offline and explain why that is actually necessary.

Joy Pritts – ONC – Chief Privacy Officer

Don't add that in right now because ... we're coming up at the end of the call, so can we have some summary before we have to open up for...?

Deven McGraw - Center for Democracy & Technology – Director

I can. Yes. I mean ... I want Micky to jump in first.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Thank you. Just one, I mean, it feels to me like we've actually come very far forward in this call, and that where we have ended up, it seems to me....

Deven McGraw - Center for Democracy & Technology – Director

I'm glad somebody thinks so.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Sorry? No, I know we didn't get as far down the agenda as you wanted, but I still believe that we're really made a lot of progress forward. It seems that we are agreeing that NHIN Direct ought to be about this line that you were talking about with no exposure to PHI with a carve out. It seems that on that point

there seems to be almost universal agreement and that the point that Dixie is raising right now is really about defining that carve out, which we knew we were going to have to get through anyway. And it seems that there may be, just to David's last point, that there may need to be a side conversation about what the technical details of that carve out are that maybe can be something that comes back to the group once we've had the side conversations that define what that carve out is, which may relate to what the definition of encryption means and how we believe it has to be instantiated in order to fulfill sort of the spirit of what we're trying to accomplish here, as well as constraining it to encryption as the only type of exposure, for example. That seems to me like it's a lot of progress.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I like the way you said that.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

That's a good summation, Micky.

Deven McGraw - Center for Democracy & Technology – Director

I do too. It's a good summation, Micky. I think you just stepped right up to the plate there.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

I thought you were going to say I stepped in it, so I'm glad you said....

Deven McGraw - Center for Democracy & Technology – Director

No, stepped right up to the plate and hit that home run. It went right over the green monster.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

And who would that be exactly?

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

I'm glad you got the right ballpark too.

Deven McGraw - Center for Democracy & Technology – Director

Yes, it's a reference to Fenway Park. There's a big green wall that is very hard to hit home runs over.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I assumed it was a sports metaphor of some kind.

Deven McGraw - Center for Democracy & Technology – Director

Paul, are you comfortable with that?

Paul Eggerman – eScription – CEO

Absolutely.

Deven McGraw - Center for Democracy & Technology – Director

Okay. So I don't know whether we dare try to get through anything else today or open the phones to the public and say we've had a good call, we're done, and we have other things to do in subsequent calls, of which there are many.

Joy Pritts – ONC – Chief Privacy Officer

I have a ... request before we do that.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Joy Pritts – ONC – Chief Privacy Officer

There are ... on this call. I don't know if either one of these people are on the call. Neil Calman and Judy Faulkner, please make your travel arrangements through VTL....

Deven McGraw - Center for Democracy & Technology – Director

Yes. This is for the technology hearing next Tuesday, for those of you who are able to attend.

Judy Faulkner – Epic Systems – Founder

This is Judy, and I have somebody in my place. I think ... travel has been sent over already.

Joy Pritts – ONC – Chief Privacy Officer

Okay. So you're not coming, and she's coming in your place. We weren't sure.

Judy Faulkner – Epic Systems – Founder

Yes, he is, and the reason I accepted is because there is a seat there, but it's ... who is taking it, and his travel has been arranged.

Joy Pritts – ONC – Chief Privacy Officer

Got it.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Deven and Paul, this is Micky. Just a question: How much more detail do you think you need for Friday? Do we need to get to this refinement that Dixie is kind of raising in terms of defining the carve out?

Deven McGraw - Center for Democracy & Technology – Director

No, I don't think we can. I think we can say that we are going to work on that piece. I think what we have to take the recommendation documents that we've been working on and put in this NHIN Direct piece that we clarified on the call today, but say that we have to work out the technical details. I just don't think we can do that in time for the policy committee meeting. It sounded like it was going to take a little bit of work, unless people are going to tell me I'm wrong about that. I think we have to put that in the very near parking lot. Maybe we'll call it the valet parking lot because it's right....

I think maybe we should do some public comment and let everyone take a breather, and we'll go from there.

W

Good idea.

Deven McGraw - Center for Democracy & Technology – Director

Again, this document is going to come back around, and you have anything to add, please try not to wordsmith it excessively, but if you've got to respond to it in some substance, you're going to need to do that, so keep an eye on your e-mail.

Judy Sparrow – Office of the National Coordinator – Executive Director

Are we ready for the public?

Deven McGraw - Center for Democracy & Technology – Director

Yes. Thanks, Judy.

Judy Sparrow – Office of the National Coordinator – Executive Director

You're welcome. Operator, can you see if we have any public comment?

Operator

Our first comment is from Fred Burr with Medi Steward.

Fred Burr – Medi Steward

My name is Fred Burr. I live outside of Madison, Wisconsin, and I would recommend that essentially that the administration on aging, their privacy officers, and other data individuals be included in future discussions. And I would like to give two illustrations of a situation that I'm involved in. I'm actually an end user, a patient essentially. One of the situations I would describe is that if I'm a cancer patient at the Carbone Cancer Center at UW, and my primary care physician is at Meriter Hospital, also here in Madison, both my medical records are separate instances, but are in Epic. My specialist can see my Epic record at Meriter, as well as my record at UW Health. She practices at both. However, my primary care physician only practices at Meriter, and she must request my UW records be faxed when I'm actually in her office.

My second illustration is because I'm a senior and participate in programs at my senior center, I'm asked, and this is on a voluntary basis, to – when I participate in a program such as living well, which is related to managing chronic care conditions, I am asked to voluntarily submit a questionnaire in which I'm asked a variety of questions in which also my chronic care conditions are itemized, such as whether I have diabetes, heart disease, hypertension, lung disease, depression, or arthritis, rheumatism, cancer, or other type of chronic conditions. Essentially the instructions say that the UW researcher will keep these records in a database in her office actually, but unknown to most people, and I only discovered this because I volunteered to enter data for our senior center is that these records are also kept in a database that is part of the agingnetwork.com database, which is host-based with Web servers in Fairfax and some places in Vermont.

These are clear text databases, and I just wanted to raise this question because it violates all my senses related to the security of the confidential information related to research. Anyway, those are the two comments that I'd like to make. Thank you.

Judy Sparrow – Office of the National Coordinator – Executive Director

Thank you, Mr. Burr. Do we have anybody else?

Operator

We do not have any more questions at this time.

Judy Sparrow – Office of the National Coordinator – Executive Director

Thank you. Just a reminder, the next call is on Monday, June 28th.

Deven McGraw - Center for Democracy & Technology – Director

No rest for the weary.

Judy Sparrow – Office of the National Coordinator – Executive Director

No. Continue on.

Deven McGraw - Center for Democracy & Technology – Director

Thank you very much, everyone.

Judy Sparrow – Office of the National Coordinator – Executive Director

Thank you.

Public Comment Received During the Meeting

1. Allowing the 'first hop' HISP and the 'last hop HISP' to have access to PHI; is just as legitimate as the 'Nth hop HISP'. The access is either needed or justified or it isn't.
2. Directed Exchange is NOT SIMPLE. The assumption that there is something called SIMPLE DIRECTED EXCHANGE is wrong. There would not be so many workgroups on this topic if it really was SIMPLE.
3. Isn't the difference between A-C the very fact that the sender and receiver have reason to need the different levels of value-add? Thus an Intermediary provides a WANTED functionality.
4. Category A is very valid. A directed communication between two parties that do not need assistance from an intermediary. Again, an Intermediary needs to be defined. An IP router provided by an ISP is not an intermediary.
5. I am concerned that the recommendations are being crafted to eliminate a large number of NHIN-Direct attendees proposed solution without a good justification.
6. Internet routers are NOT Intermediaries.
7. There is only an Intermediary shown when there is some legitimate (and well known) translation necessary.
8. There are NHIN-Direct solutions that require NO intermediaries!
9. HIPAA already has overall guidance that is scalable and appropriate!
10. The RECEIVER can and must be allowed to retain the data!
11. Why are you forbidding the Sender from deciding how the directed communication is used? If the sender has authorization, why can't they directly communicate?